Guideline

Official

Subscribe to Release Notification

Reliability Analyses for Flight Hardware in Design, Rev. 2

Doc ID: 34904	**DocRevID:** 80729	**Doc Code:** D-5703	**Effective Date:** 11/27/2001
Doc Owner: Clawson, James	**Process:** Assure Product Reliability	**Process Owner:** Greanias, George	**Next Review Date:** 5 year(s) after publication
Revision 2: In this revision, as per the process owner's request, document type changed from Handbook to Guideline, and title changes from "Reliability Analyses Handbook," to "Reliability Analyses for Flight Hardware in Design."			

Foreword

Revision 1 of the **RELIABILITY ANALYSES HANDBOOK** deletes obsolete information while incorporating the latest technical information, including formatting rules of Document 45292; "Formatting Specification for Documents Submitted to the DMIE Information System". Furthermore, **an overview of the PRA is given in paragraph 3.8 of this document.** A process containing a value added tool for performing a detailed Probabilistic Risk Assessment (PRA) is under development in the Reliability Engineering Office.

Code Q of the NASA program and Project Responsibilities for Safety and Mission Success now requires the use of a formal risk management process, risk management technologies (e.g., failure modes and effects analysis, fault tree analysis, and probabilistic risk assessment), and design for safety on all NASA programs and projects. The scope of early planning and implementation of these requirements by programs and projects can also be viewed at http://www.hq.nasa.gov/office/codeq/sms.pdf. The point of contact for this activity at NASA Headquarters is: Dr. Michael G. Stamatelatos, Code Q; (202) 358-3300.

It is strongly recommended that the applicable reliability analyses activities be accomplished using guidelines provided in this document. Guidelines for the selection of appropriate reliability analyses to ensure proper built-in reliability can be found in section 4.0 of the JPL Standard for Reliability Assurance, **JPL D-8671/DMIE ID # 34905**.

Questions and/or comments regarding this document should be sent to Krishna K. Sinha or to the office manager and process/document owner James F. Clawson.

1.0 Introduction

1.1 General

This handbook provides guidelines for performing and reviewing reliability analyses for flight hardware in design. The analysis guidelines contained in this document is responsive to the requirements of D-8671; "JPL Standard for

Reliability Assurance", as referenced in DBAT Policy statement in paragraph 6.0. This document also provides procedures for identifying, preparing, processing, tracking and resolving deficiencies in the analyses and/or design. This document does not address analyses required in direct response to safety concerns.

It should be understood that these analyses are not an after-the-fact documentation of what resulted from the design process, but are an active integral part of the design process. An immediate action is warranted by the project-designated individual should an unacceptable analysis result be found, the project should be notified.

1.2 Purpose

The analyses guidelines provide a centralized source of information on performing and reviewing reliability analyses. The purpose is to promote uniformity of the various methodologies, both within a specific project and from project to project. The review guidelines not only provide information to assist the review function, but by explicitly defining what the reviewer should be looking for, the analyst performing the analysis can provide the information in a form that is understandable to the reviewer.

1.3 Scope

The analyses guidelines provided in this document are primarily intended for use on hardware used by projects or tasks developing flight equipment. The guidelines may be used for other projects or tasks, if such analyses are appropriate or required.

1.4 Applicability

The procedures and guidelines provided in this document are applicable to JPL projects/tasks, either in-house or system contractor mode.

1.5 Design Approach

Risk management of flight systems requires inputs from many disciplines. The role of reliability design analyses is to provide quantitative risk assessment data in support of the risk management process. For this process to be effective, the design analyses must be consistent and based on reasonable assumptions. For example, the part stress analysis (PSA), the worst-case performance analysis (WCA), and fatigue life of mechanical elements (solder joints, connectors, etc.) are all based on a thermal analysis of the electronics.

These thermal analyses should be based on the project required qualification test mounting surface temperatures and used for both parts stress and WCA. The methodology for thermal requirements is defined in Section 3.2 of Appendix B of this document. Fatigue life is based on worst-case expected test/mission cycles and ranges. The fatigue estimated life analyses and special test requirements are an Office of Reliability Engineering responsibility as is a fatigue margin analysis report. Inadequate life items will be reported on a DDR form, or equivalent, and pursued with the Project for corrective action.

Because all of the "reliability" analyses tend to be interwoven, they should utilize a common dataase comprised of realistic assumptions and estimates and be initiated in the conceptual design phase. It is required that these reliability design analyses be completed and independently reviewed prior to the CDR.

This approach requires good thermal design practices to assure that piece part junction temperature limits are not exceeded when module/assembly base-plate are designed and tested to levels corresponding to the above thermal control mounting surface temperature levels. Further, this approach provides the required in-flight thermal margin to assure low thermal stress and the consequent low failure rates, which translate to high reliability. In addition, it assures that the design will provide "in-spec" operation at the various thermal levels.

Analysis verification testing is a very important element in the reliability design analyses process. For example, thermal survey mapping testing significantly improves the system development/qualification cycle by providing vital feedback to the reliability design analyses process.

In summary, the quality of reliability design analyses is significantly increased when worked in a coordinated manner, using realistic assumptions and estimates, and when verification testing is part of the qualification procedure.

2.0 General Requirements

This section addresses issues that are applicable to all analyses performed in support of flight equipment design and development. If specific analyses have unique requirements, they are addressed within the detailed guidelines provided in the appendices.

2.1 Formal Documentation Requirements

Flight equipment design and development efforts utilizing reliability analyses should document them as outlined below. Formal documentation is an activity essential to recording the design capabilities for subsequent review during operation (i.e. test or flight) and to make the analysis readily available for independent review or audit. It should be stressed that "formally documented" does not mean edited, printed and bound report with artwork, etc. The criteria are completeness and correctness coupled with trace-ability and legibility to enable peer review (e.g. legible hand printing is acceptable). To this end, each analysis report should, as a minimum, contain the following elements:

1. Title Page
2. Applicable Documents
3. Functional Descriptions
4. Performance Requirements
5. Analysis Assumptions and Boundary Conditions
6. Analysis Model
7. Software Analysis Tool(s) Description
8. Analysis Results
9. Summary and Conclusions

Each of these elements is described in the subsequent paragraphs.

1. Title Page

The title page shall provide the following information:

- Project Name
- Project Number
- System/Subsystem/Assembly/Circuit Names
- Analyst Name and Signature

- Date Analysis Completed
- Independent Reviewers Name and Signature
- Date Independent Review Completed
- A unique Analysis Identification Number

2. Applicable Documents

All documents that apply in the performance of the analysis should be cited in this section of the report. Specifically, all documents that contain requirements (functional, interface or environmental) that the analysis is to validate should be cited. All documents including circuit schematics, drawings, specifications or policy documents used and referenced in the analyses should be included here. Document identifications should include:

- Document Name or Title
- Document Number
- Revision Number/Letter
- Release Date
- Issuing Organization

3. Functional Description

The hardware function should be clearly explained, including interfaces with other hardware and/or software items. The theory of operation should be explained in plain language, avoiding numerical values and detailed specific facts as much as possible. The discussion should provide an overview of the hardware operation. It should be provided at a level of detail consistent with the analysis being documented in the report. The discussions shall be supplemented with a block diagram that illustrates the functional relationship of the elements that make up the hardware being analyzed. Each functional element shall be identified and its interface with other elements, both internal and external to the hardware being analyzed, accurately depicted.

4. Performance Requirements

The specified and/or derived requirements for the hardware should be identified in this section. Specified requirements are those imposed directly on the hardware, whereas derived requirements are indirect as they are passed down from a higher level through other hardware or by other requirements. The requirements should be presented in matrix format. The matrix should list the requirement parameters on one axis of the matrix and the source of the requirement on the other. The actual requirement (i.e. the specified value) is entered in the matrix cell corresponding to the parameter row and the requirement source column. The specified value becomes the acceptance criteria for the analysis. All documents cited as sources of requirements/acceptance criteria shall be included in the Applicable Documents section, described above.

5. Analysis Assumptions and Boundary Conditions

All analysis assumptions shall be clearly identified, including boundary conditions for the analysis. These may include simplifying conservative assumptions that make the analysis tractable and/or more cost effective. Boundary conditions may include physical or functional interfaces with other elements or hardware. It may also be a limitation on the number of functions modeled. Where functions are not analyzed, the rationale for that decision must be documented.

6. Analysis Model

This section shall describe the analysis methodology and the rationale for its use in proving that the hardware design is satisfactory (i.e. positive margins for all functional requirements). The methodology shall be fully described. This may be a "stand alone" description, or it may reference other available documentation. This other documentation may be the specific guidelines provided in this document, or it could be the theory manual of a mature computer program.

7. Software Analysis Tool Description

If software is used in the analysis it must be appropriately referenced. If mature software (i.e. a program that is fully developed, tested and documented) is used for the analysis, it is sufficient to reference the documentation (including source and version), if it is readily available to technical peers.

If software is specifically developed for the analysis of the subject hardware, it must be fully documented and tested. The documentation shall include the theory of operation and logic flow charts depicting its operation. The documentation shall also include a user's guide and a listing of the program. The validity of the program shall be demonstrated by documented test cases which indicate the accuracy of the program and the limits of operation. The limits of operation define the range of input parameters over which the program provides reliable output and/or over which the program has been tested.

8. Analysis Results

The results of the analysis shall be documented in this section. Where feasible, the results should be presented in matrix format with both the analysis results and requirement/acceptance criteria presented side-by-side. Any deviation from the requirement/acceptance criteria shall be clearly identified. In addition, any explanation as to why the deviation occurred and/or how it can be corrected shall also be provided.

9. Summary and Conclusion

This section shall provide a summary of the analysis results. If the analysis indicates that the hardware performance is expected to be within the performance requirements, this should be explicitly stated. If possible, the margin above the required performance should be stated.

Likewise, any and all expected deviations from the required performance that are revealed by the analysis shall be pointed out in this section. The extent and significance of the deviation should be assessed and any proposed solutions identified. In addition, any departure from the acceptable analysis methodologies and/or required environments shall be reported. Note: Any deviation from the performance requirements and/or analysis methodology must be approved.

2.3 Inherited Hardware Analyses

The first step in the assessment of analyses of inherited hardware is to establish if the required analysis was performed for the prior application and, if performed, how it was documented.

If prior analyses are available, the applicability of the prior analyses to the new use must be assessed. This assessment should determine if there have been any significant changes in the requirements and/or the design from the prior to the current application. It is not intended to require extensive new analyses of inherited designs if such analyses were previously performed to requirements that meet or exceed the new project requirements. Therefore, every reasonable effort should be made to demonstrate the applicability of the prior analyses.

If it is established that the prior analyses are applicable, the technical adequacy of the analyses can be assessed using the appropriate checklist (i.e. FMECA, WCA, etc.) given in Section 4.0. If the prior analyses are not available or are considered technically inadequate, the analyses must be redone or revised to meet the requirements of the current application.

2.4 Independent Review Criteria

The independent review of analyses constitutes review of the analyses by such individuals who have had no part in generating the analyses and generally from a different organization. Independent review of analyses is conducted by individuals with expertise to generate such analyses. When the original analysis is performed by a JPL technical division, it is reviewed by the JPL Project Reliability Group. If, on the other hand, an analysis was performed by the Project Reliability Group, the cognizant technical group is responsible for conducting the independent review. When analyses are performed by a contractor, the independent review may be conducted by either or both the JPL cognizant technical group and/or the Project Reliability Group. In any case, the reviewer is required to document the findings of the review in a memo, as described in Section 5.0 of this document.

Review guidelines and checklists for each type of analysis are provided in Section 4.0 of this document.

2.5 Waivers

This document provides a uniform and consistent interpretation of analyses for use during the design and development of JPL flight equipment. The waiver system is to be employed where differences exist between the actual performance and the technical requirements. These differences can develop in a number of areas, including, but not limited to:

1. Decisions not to perform a required analysis;
2. Decisions to accept out-of-spec performance under some analyzed mode of operation;
3. Departures from the analysis methodology, including the approach, environments, interfaces and/or derating criteria;
4. Decision not to have analyses independently reviewed.

The waiver procedure and signoff is to be in accordance with JPL Waiver policy of the affected project using JPL Waiver request and approval forms JPL-1993-S or JPL-1994-S as applicable.

3.0 Analyses Overview

The design of space-flight hardware involves many steps to ultimately result in reliable performance. Some of these steps include a selective parts, materials and processes program, an intense system engineering activity, conservative design practices by the technical divisions, adversarial design review by technical peers, thorough testing at all levels of hardware (including the flight system), and design validation by analysis. The latter item, design validation by analysis, is the subject of this document. This process, to be effective, is started as early as possible and continues throughout the design development. The basic design philosophy is to develop flight systems that not only have redundancy, but also have partial survival capabilities under failure conditions of the primary hardware. Various analysis techniques are used to validate functionality of the hardware under various conditions, including the following: failures, extreme conditions and end of life. Table 3.0 groups this data into a matrix of analysis type versus conditions. It can be seen that most analyses validate functionality under one specific set of conditions; thus, for complete design validation, all analysis types need to be performed. The following paragraphs provide a brief overview of each type of analysis and more details on the benefits derived from each.

TABLE 3.0 Design Validation Matrix - Analysis

	Functionality under Failures	**Functionality under Extreme Conditions**	**Functionality for long life**
FMECA	X		
Redundancy verification analysis	X		
WCA	X		X
EEE Parts Stress			X
FTA	X		
SEE		X	
Parameter trend analysis			X
PRA	X	X	X

3.1 Failure Modes, Effects and Criticality Analysis (FMECA)

FMECA is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations. The analysis is sometimes characterized as consisting of two sub-analyses, the first being the failure modes and effects analysis (FMEA), and the second, the criticality analysis (CA). The FMEA addresses all postulated part failure modes in a system and the resultant effect on its operation. The CA ranks each postulated failure mode according to the criticality of the effect on system operation and the probability of its occurrence. Successful development of an FMEA requires that the analyst include all significant failure modes for each contributing element or part in the system. FMEAs can be performed at the system, subsystem, assembly, subassembly or part level. In general, failures to start/stop, open/close or continue to operate should be considered.

FMECA should be a living document during development of a hardware design. It should be scheduled and completed concurrently with the design. If completed in a timely fashion, the FMECA can help guide design decisions. While the FMECA identifies all part failure modes, its primary benefit is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design modification at the earliest point in the development effort. Hence, the FMECA should be performed at the system level as soon as preliminary design information is available and extended to the lower levels as the detail design progresses. The analysis may be performed at the functional level until the design has matured sufficiently to identify specific hardware that will perform the functions; then the analysis should be extended to the hardware level.

When performing the hardware level FMECA, interfacing hardware is considered to be operating within specification. In addition, each part failure postulated is considered to be the only failure in the system (i.e., it is a single failure analysis). In addition to the FMEAs done on systems to evaluate the impact lower level failures have on system operation, several other FMEAs are done. Special attention is paid to interfaces between systems and in fact at all functional interfaces. The purpose of these FMEAs is to assure that irreversible physical and/or functional damage is not propagated across the interface as a result of failures in one of the interfacing units. These analyses are done to the piece part level for the circuits that directly interface with the other units. The FMEA can be accomplished without a CA, but a CA requires that the FMEA has previously identified system level critical failures. When both steps are done, the total process is called a FMECA.

Major benefits derived from a properly implemented FMECA effort are as follows:

1. A documented method for selecting a design with a high probability of successful operation and safety.

2. A documented uniform method of assessing potential failure modes and their impact on system operation, resulting in a list of failure modes ranked according to the seriousness of their system impact and likelihood of occurrence.

3. Early identification of single failure points (SFPS) and system interface problems, which may be critical to mission success and/or safety. They also provide a method of verifying that switching between redundant elements is not jeopardized by postulated single failures.

4. An effective method for evaluating the effect of proposed changes to the design and/or operational procedures on mission success and safety.

5. A basis for in-flight troubleshooting procedures and for locating performance monitoring and fault-detection devices.

6. Criteria for early planning of tests.

From the above list, early identifications of SFPS, input to the troubleshooting procedure and locating of performance monitoring/fault detection devices are probably the most important benefits of the FMECA. In addition, the FMECA procedures are straight-forward and allow orderly evaluation of the design. A computer program can be very useful in performing circuit FMECAS, since there may be a large number of computations and a large amount of record keeping required for hardware of reasonable size. Ideally the FMECA program would have two main features; first, it would analyze circuit performance under the condition of each piece part failure mode, and secondly, it would have database features that would record the failure mode and the resulting next higher-level performance impact. Once these steps are completed, the database function would allow editing of the database to identify corrective action planned or implemented to mitigate the affect of the failure. In addition, the criticality rating and probability of occurrence can be added to the record when they are established. Once the analysis results are in the FMECA database, it can be rank sorted to focus attention on the most critical items.

3.2 Redundancy Switching Analysis

This analysis is performed to verify that if a failure of a redundant system element occurs, the source of that failure is appropriately detected and that mechanisms exist and are capable of reliably operating to affect a switch to the redundant system element to continue system operation. In designs utilizing autonomous in flight fault detection and correction schemes, this analysis can be a subset of a large system engineering fault correction study.

Although there may be other acceptable ways of performing this analysis, the FMECA format and methods lend themselves to this task effectively.

3.3 Worst-case Analysis

Worst-case Analysis (WCA) is an extension of classical circuit analysis, but uses a different approach and has a different objective. The most significant difference in the approach is the use of part parameter data and conditions at their extreme values rather than the nominal value. In the WCA, the classical circuit analysis is repeated for the worst combination of extreme values of part parameters and conditions. Thus, to assure reliable performance of spacecraft circuits, it is essential that variations in these parameters and conditions be addressed as the circuit design is developed. The "Worst-case Analysis" methodology has been developed over the years to address these effects for both analog and digital circuits and is briefly described below

To facilitate the performance of the WCA, the analyst reduces complex circuits to smaller functional blocks aiding both the analyst and the reviewer. Performance requirements for each block need to be established, defining both inputs and outputs. These requirements will serve as the evaluation criteria for the WCA results for the functional blocks. Requirements for some functional blocks will have to be derived from higher-level specification requirements. The WCA should show compliance with all requirements, both on the functional block level and at the circuit level. Proof of compliance to certain less significant requirements may be omitted provided that adequate justification for the specific omission is given. The remainder of this discussion will refer to circuits, but is intended to apply to the lower level functional blocks also.

The worst-case conditions of any given circuit will be a combination of the extreme values of the following factors:

1. Circuit interface inputs and loads
2. Piece part parameter variations

These factors are described in the following paragraphs.

The inputs to the circuit are taken to their specified maximum and minimum voltage, time and/or frequency with the intention of driving the outputs of the circuit to their maxima and minima. The variations of signals presented to the circuit being analyzed are to be those continuous values that are applied at the inputs to the circuit. If the circuit is a control circuit that feeds back, in effect, to its own input (e.g., a regulator circuit), it is subject to the limits of its control range in the WCA. Likewise, the interface characteristics on the circuit's output side (i.e. loads, etc.) are also to be taken to the appropriate maximum or minimum extreme.

The total parameter variation depends on variations resulting from a number of causes. The worst-case variation for any one-part parameter is the product of the individual parametric variations, as follows:

$(1+dP) = (1+dX)(l+dS)(l+dT)(l+dE)(l+dR)$

where: dP is the total parametric variation

dX is the part initial tolerance

dS is the variation due to aging and drift

dT is the variation due to piece part case temperature (worst-case direction)

dE is the variation due to applied voltage and frequency

dR is the variation due to radiation degradation

The analysis is a true worst-case in that the value for each of the variable part parameters will be set to limits that will drive the output(s) to a maximum or minimum or both, depending on the circuit function. Piece-part temperatures are derived by a detailed thermal analysis starting from the shear plate design temperature levels.

In many cases (e.g., RF circuitry), the modeling and analysis of a circuit may prove to be extremely difficult and questionable for certain parameters. In these cases, it may be expedient to use laboratory test data in conjunction with analysis to determine the worst-case response. For those parts that are difficult to model, the laboratory test is used to establish the part parameter sensitivity which can be used in a simplified analysis to achieve all worst-case conditions.

3.4 EEE Part Stress

Electronic parts are prone to premature failure due to overstress, especially thermal. Certain parts are more stress sensitive than others. Decreases in failure rate can be achieved by reducing part stress levels. Derating is the procedure of requiring parts to operate at stress levels below the manufacturer's rated values. Derating procedures vary with different types of parts and their application. Resistors are derated by decreasing the ratio of operating power to rated power. Capacitors are derated by maintaining the applied voltage at a lower value than the voltage for which the part is rated. Semiconductors are derated by keeping the junction temperature below a defined value. Derating electronic parts involves the use of derating equations and curves found in JPL D-8545.

3.5 Fault Tree Analyses

The Fault Tree Analysis (FTA) is characterized by a fault tree diagram. The diagram is a logic diagram depicting an undesired or failed state of the system at the top of the tree (FT) with underlying branches of the FT representing subsystem and component failures that can lead to the undesired or failed state ("TOP EVENT"). Depending on the system configuration (i.e. redundancy, level of fault tolerance, etc.), one or more subsystem or component failures may be required before the Top Event occurs. For example, if failure of two redundant components is required to cause the Top Event, their failures would be depicted as input to a logical "AND" symbol. Likewise, if failure of any one of a series of components would result in the Top Event, their failures would be depicted as input to a logical "OR" symbol. Both of these logic symbols would be a direct input to the Top Event. Generally, the system FT is constructed with failures of the major functional element (say the subsystem) depicted as the first level below the Top Event, then failure of the next lower functional element depicted as the second level below the Top Event. This process can be carried down to the lowest level of element for which failure information is available or can provide the detail required of the analysis. An example of a simple block redundant system is depicted in Figure 3-1. An example of a simple single string (or series) system, consisting of five subsystems, is depicted in Figure 3-2.

A companion FT prevention matrix is developed and addresses the possible corrective actions, including design changes, inspections or other product assurance activities that the project could implement to eliminate or minimize each of the identified failure modes.

At JPL, the FTA has traditionally been applied to mechanical and electromechanical systems; however, there is no fundamental reason why the FTA methodology could not be applied to any type of equipment. **Use of mission level FTA’s is strongly recommended for all Projects. Mission level FTA’s should be considered by projects early and throughout the life cycle of the project for risk assessment as part of the overall risk management activities.** There are practical reasons, why it is not feasible to apply the methods to electronic equipment at the piece part level, and one is the large effort that would be required. In most cases the benefits would not warrant the effort. These evaluations are more economically handled by other methods, such as FMECAs. These latter methods do not provide the easy visual interpretation available with the FT logic diagram nor do they address potential multiple failures, but are considerably less labor intensive.

The FTA handbook NUREG-0492 provides a detailed methodology for constructing and reviewing fault trees and is published by NTIS, US Department of Commerce.

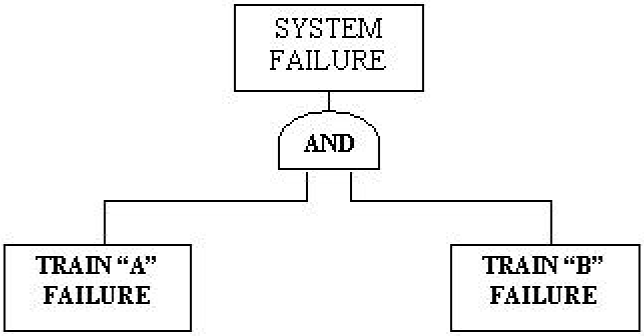


Figure 3-1 Fault Tree For Simple Redundant System

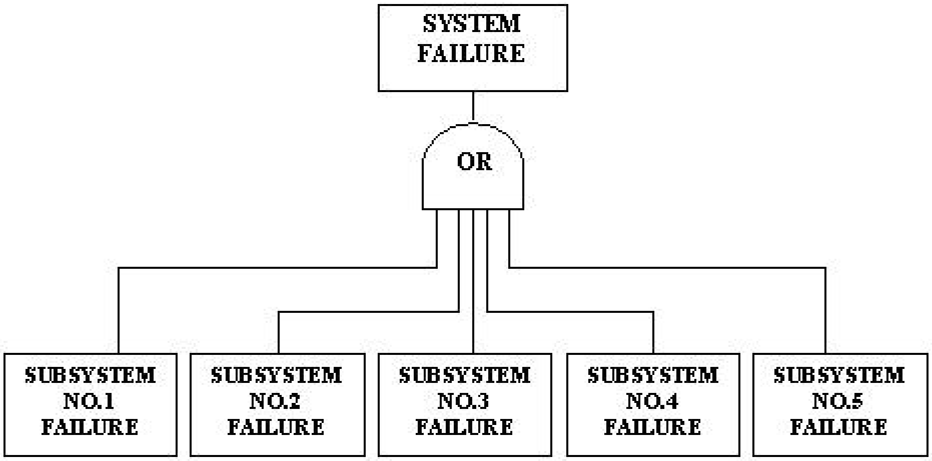


Figure 3-2 Fault Tree For Simple String (or Series) System

3.6 Single Event Effects (SEE) Analyses

Single Event Effects (SEEs) occur in microelectronics when a single particle, usually a heavy ion or proton, deposits enough charge at a sensitive node in a circuit to cause a change of electrical state. Heavy ions and protons are found in galactic cosmic rays, solar flares and in radiation belts around planets. SEEs may include any of the following four effects:

Transient Output:

The energetic particle may deposit enough energy to generate a sub-micro sound output transient that could cause erroneous triggering of a high high-speed following stage. A system transient analysis should be performed for sensitive circuits to verify that no irreversible functional actions are taken or that any down time is mission tolerable.

Device Latch up:

Certain electronic devices can experience state changes that require power removal to unlatch, requiring either sophisticated autonomous fault protection or ground intervention. Most projects categorically exclude such devices, but special analysis may be required if the part use is mandatory (no alternative).

Device or Circuit Burn Out:

When a latched up device exists in a circuit without adequate current limiting, burn out of the device or other circuit parts can result. Analyses may be required to assure that the limiting maintains all circuit devices within the stress derating limits.

Single Event Upsets:

SEUs became a concern in the late 1970's because advancing technology (both CMOS and bipolar) evolved towards lower power and higher speed; consequently a smaller amount of charge on a circuit node was used to store, information. The charge magnitude required to cause a state change depends upon the electronic part, technology, and size. SEUs are produced in an integrated circuit when a particle produces a change of state (1,0) in one or more memory locations within the chip. A memory location is typically made up of more than one active device and connecting components.

The SEU analysis consists of four steps, as follows:

1. Define the radiation environment (fluence vs. energy).
2. Identify the SEU sensitive electronic parts by means of critical LET and cross section analysis or measurements (energy upset threshold)
3. Combine the information from the first two steps (1 and 2) to predict the upset rate for each sensitive part.
4. Perform a circuit (system) response analysis using the above information to provide number of upsets per unit time, effects on operation, mission criticality, and, when applicable, percentage of data loss due to particular upsets.

Note that the primary responsibility for SEE analyses rests with the circuit and system designers and the parts engineers and physicists. The reliability engineering will provide or review analyses only after specific requests from these organizations.

3.7 Parameter Trend Analyses

When a limited life or consumable item is to be used in flight, both pre-launch and mission decisions can be aided by a Parameter Trend Analysis (PTA). If the mean life expectancy is less than five mission lifetimes, the consumable is a candidate for PTA.

The methodology of the analysis as follows:

1. Define EOL (End of Life) criteria for the critical parameter variable (i.e. gas volume, RF & DC power, etc.
2. Assure that adequate spacecraft instrumentation exists to accurately measure the parameter.
3. Measure the parameter periodically from EOL through pre-launch and extrapolate the aging trend.
4. Define an acceptable minimum pre-launch EOL prediction and flag any device that ages too rapidly for possible pre-launch replacement.

5. If acceptable at pre-launch, continue flight measurements and predictions. Report premature aging to the project for possible action.

Example: Traveling wave tubes (TWT) have a finite lifetime, rarely longer than three mission lifetimes. For this reason they are usually employed redundantly. If TWT power is falling off prematurely, the project has several alternatives. The optimum coarse of action will be related to the rate of fall off, such as:

a) Turn on B and hope that A shows recovery

b) Try to communicate with A at lower than spec power at increased data error rates.

c) Reduce the communication duty cycle and lose some data.

d) Increase the filament voltage to A, trading power for life.

Responsibility: Project reliability has the obligation to unilaterally identify candidates early in the design phase and recommend parameters as candidates for PTA. If a recommendation is concurred by the project management, project reliability would perform steps one through five and periodically report the status.

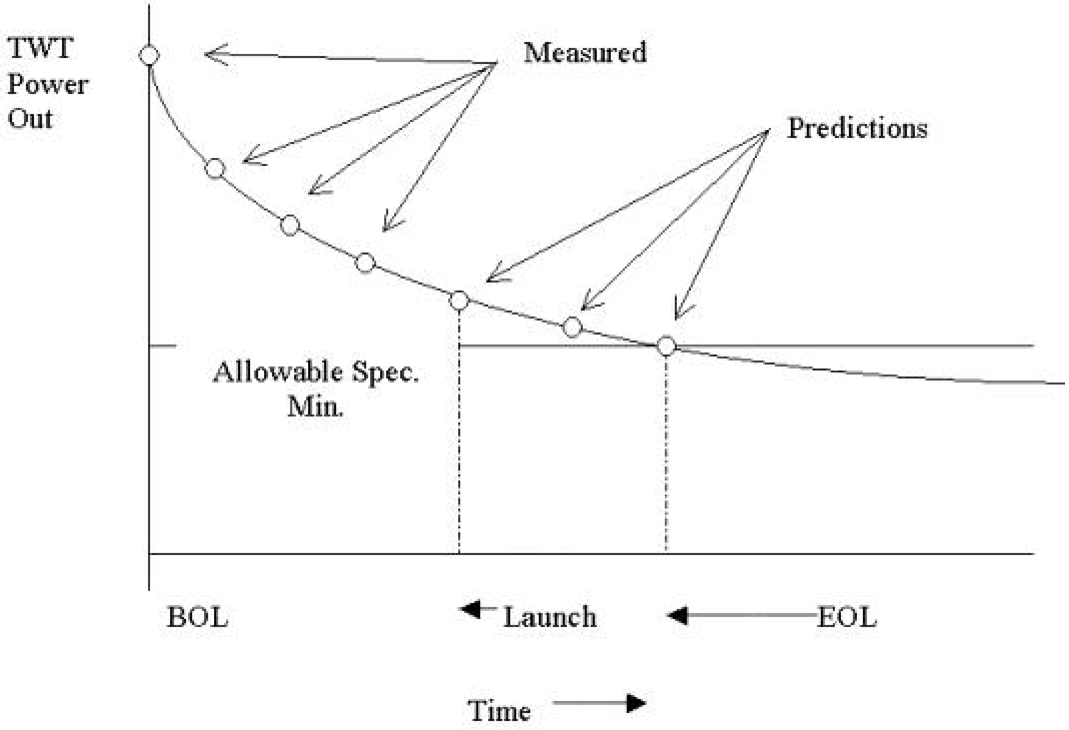


Figure 3.3 TWT Power Parameter Trend

3.8 Probabilistic Risk Assessment

PRA is an analysis of the probability (or frequency) of occurrence of a top-level undesired event, including an assessment and display of our degree of uncertainty surrounding the probability. It is based on comprehensive systems analysis and is repeated periodically as the design matures and new data become available. PRA can be used to support strategic decision making such as in answering the question “What is the probability of losing flight hardware during its assembly and operations?” For systems under development, PRA provides a basis for tradeoffs among safety, reliability, cost, performance, and other resources. For mature systems, it can be used for decision making on risk acceptability, and, when risk is considered to be too high, choosing among options for risk reduction.

PRA may also be used to track risk levels throughout the life cycle of an program/project. While FMEAs, FTAs, PRAs, and other safety and mission success methods are best applied early, they can provide useful results when applied at virtually any time during the program/project life cycle. PRA is an evolving technical capability which involves estimation of the degree or probability of loss. A formal definition proposed by Kaplan and Garrick (1981) is a useful description of the elements of probabilistic risk assessment which involves addressing three basic questions:

1. What can go wrong that could lead to hazardous exposure?
2. How likely is this to happen?
3. If it happens, what consequences are expected?

To answer question 1 would be a list of scenarios of events leading to the outcome. The likelihood of these scenarios should be estimated and the consequences from each be described. Hence, risk “R” can be quantified as follows in the equation below:

$$R = \langle S_i, F_i, C_i \rangle \text{ for I} = 1, 2, \ldots n$$

Where:

S_i = scenario of events that lead to hazard exposure

F_i = likelihood or frequency of scenario $S_{i,}$ and

C_i = the consequence or evaluation measure of S_i, e.g., a measure of the total loss

Since the above equation involves an estimation of the likelihood of occurrence of events, the PRA includes estimation of the performance i.e., reliability of the safeguards system. Furthermore, a systematic identification of scenarios may involve the use of system analysis techniques such as fault tree analysis.

The results of the risk assessment are used to determine the importance of undesirable outcomes of the activity and make decisions about the situation that would reduce the likelihood of the outcome and/or the consequence of the occurrence. On NASA programs and projects, risk management is balancing risk with cost, schedule, and design for safety. It consists of risk identification, risk assessment, decision making of the disposition of risk (accepting, tolerance through waivers, or mitigation), and tracking the effectiveness of the results.

A detailed approach to PRA is currently under development in JPL Office of Reliability Engineering and will be added to this document as an appendix when completed and approved.

3.8.1 Formalization of Risk Assessment

Since the risk assessment process focuses on scenarios that lead to hazardous events exposure, the general methodology becomes one that allows the identification of all possible scenarios, calculation of their individual probability or frequency, and a consistent description of the consequences.

3.8.2 Steps in Conducting a PRA

A) Methodology Definition

Preparing for a PRA begins with a review of the objectives of the risk analysis. An inventory of possible techniques for the desired analysis should be developed. The available techniques range from required computer codes to facility experts and analytical experts. Modarres (1993), and Henely and Kummamato (1996) are good references for the inventory of methodological approaches to PRA.

Figure 3.4 shows the general PRA process. Specific PRA steps are described below.

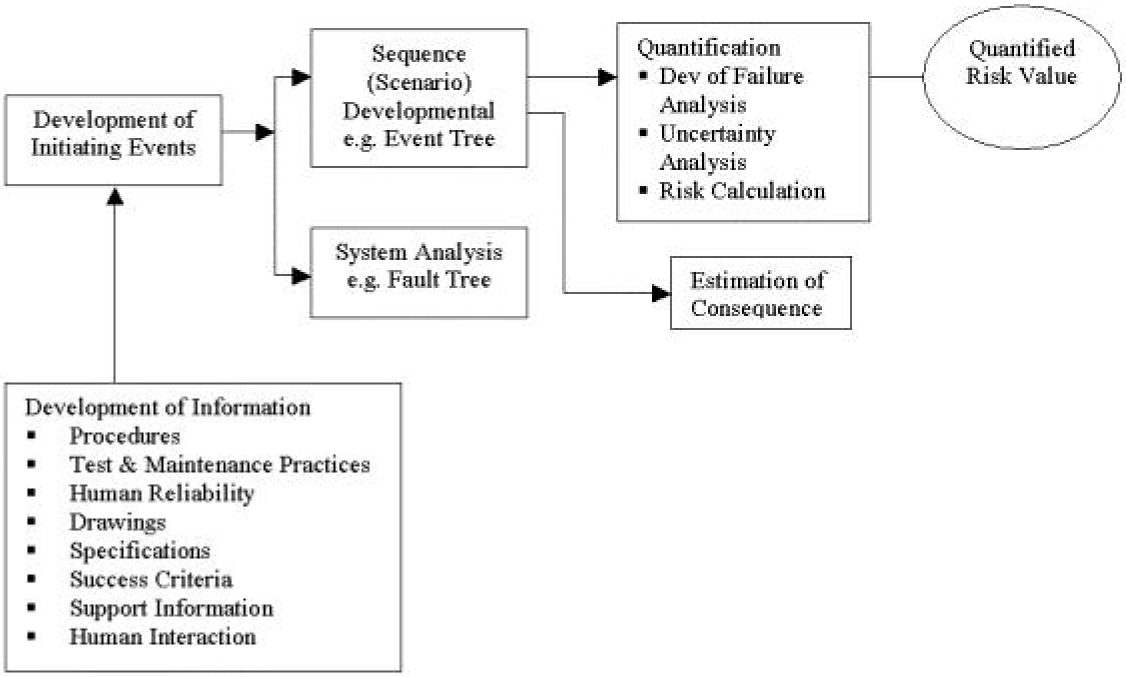

Development of Initiating Events
Sequence (Scenario) Developmental e.g. Event Tree
System Analysis e.g. Fault Tree
Quantification
▪ Dev of Failure Analysis
▪ Uncertainty Analysis
▪ Risk Calculation
Quantified Risk Value
Estimation of Consequence
Development of Information
▪ Procedures
▪ Test & Maintenance Practices
▪ Human Reliability
▪ Drawings
▪ Specifications
▪ Success Criteria
▪ Support Information
▪ Human Interaction

Figure 3.4 The Process of Probabilistic Risk Analysis (PRA)

The resources required for each analytical option should be evaluated, and the most cost-effective option selected. The basis for the selection should be documented briefly, and the selection process reviewed to ensure that the objectives of the analysis will be adequately met.

B) Familiarization and Information Assembly

A general knowledge of the physical layout of the system or process (e.g., facility, plant, device), administrative controls, maintenance and test procedures, and protective systems whose function maintains safe operation and general safety is necessary to begin the PRA. All systems, locations, and activities expected to play a roll in the initiation, propagation, or arrest of an upset or hazardous condition must be understood in sufficient detail to construct the models necessary to capture all possible scenarios.

The main elements of this step are:

1. Major protective, mitigative, safety and emergency systems (or methods) should be identified.
2. Physical interactions among all major systems should be identified and explicitly described. The result should be summarized in a dependency matrix.
3. Past major failures and abnormal events that have been observed should be noted and studied. Such

information would help ensure inclusion of important applicable scenarios.

4. Consistent documentation is key to ensuring the quality of the PRA. Therefore, a good filing system must be created at the outset, and maintained throughout the study.

With the help of designers, operators, manufacturers, or owners, the ground rules for the analysis, the scope of the analysis, and the configuration to be analyzed should be determined. The faults and conditions to be included or excluded, the operating modes of concern, the freeze date design, and the hardware configuration on the design freeze date should also be determined. The freeze date is an arbitrary date after which no additional changes in the design and configuration will be modeled. Therefore, the results of the PRA are only applicable to the process at the freeze date.

C) Identification of Initiating Events

This task involves identifying those events (abnormal events) that could, if not correctly responded to, result in hazard exposure. The first step involves identifying sources of hazard and barriers around these hazards. The next step involves identifying events that can lead to a direct threat to the integrity of the barriers.

A system or a process may have one or more operational modes which produce its output. In each operational mode, specific functions are performed that result in the output. Each function is directly related to one or more systems that perform the necessary functional actions. These systems, in turn, are composed of more basic units (e.g. components) that accomplish the objective of the system. As long as a system is operating within its design parameters, there is little chance of challenging the system boundaries in such a way that hazards will escape those boundaries. These operational modes are called normal operation modes.

During normal operation mode, loss of certain functions will cause the process or system to enter an off-normal condition. Once in this condition, there are two possibilities. First, the state of the process could be such that no other function is required to maintain the process or system in a safe condition (safe refers to a mode of operation where the chance of exposing hazards beyond the process boundaries is incredible). The second possibility is a state wherein other functions are required to prevent exposing hazards beyond the system or process boundaries. For this second possibility, the loss of a function is an initiating event. Since such an event is related to the operating equipment, it is called an operational initiating event.

Our method for determining the operational initiating events begins with first drawing a functional diagram of the process. From the functional diagram, a hierarchical relationship is produced with the process or system objective being a successful completion of the desired output. Each function can then be decomposed into its systems and components can be combined in a logical manner to represent success of that function (Figure 3 illustrates this hierarchical decomposition). Potential initiating events are the failures of particular functions, systems, or components, the occurrence of which causes the process to fail. These potential initiating events are grouped such that members of a group require similar process system and safety system responses to cope with the initiators. These groupings are the operational initiator categories.

An alternative to the use of functional hierarchy for identifying initiating events is the use of Failure Mode and Effect Analysis (FMEA). The difference between these two methods is noticeable, namely, the functional hierarchy method is deductive and systematic, whereas FMEA is inductive and intuitive. The use of FMEA for identifying initiating events consists of identifying failure events (modes of failure) whose effect is a threat to hazard barriers. In both of these methods, one can always supplement the set of initiating events with generic initiating events (if known). For example, see NUREG/CR-4550 (1990) for these initiating events for nuclear reactors.

Events that cause off-normal operation of the process and require other systems to operate to maintain process materials within their desired boundaries, but are not directly related to a process, system, or component, are nonoperational initiating events. Nonoperational initiating events are identified with the same methods used to identify operating events. However, the events of interest are those that are primarily external to the process. These are discussed later.

The main elements of this step are:

1. Select a method for identifying specific operational and nonoperational initiating events. Two representative methods are functional hierarchy and FMEA. If a generic list of initiating events is available, it can be used as a supplement.
2. Using the method selected, identify a set of initiating events.
3. Group the initiating events such that those having the same effect on the process and requiring the same mitigating functions to prevent hazard exposure are grouped together.

D) Sequence of Scenario Development

The goal of scenario development is to derive a complete set of scenarios that encompasses all of the potential propagation paths that can lead to loss of confinement of the hazard following the occurrence of an initiating event. To describe the cause and effect relationship between initiating events and the event progression, it is necessary to identify those operational functions (e.g., safety functions) that must be maintained to prevent loss of barriers. The scenarios that describe the functional response of the process to the initiating events are frequently obtained by using an event-tree. The event tree development techniques are discussed in references Modarres (1993), Kumamoto and Henley (1996), and PRA Procedures Guide (1982).

Event trees order and depict (in approximately chronological manner) the success or failure of key mitigating actions (e.g., hardware and software operations, human actions, or mitigative hardware that automatically responds) that are required to respond following an initiating event. In PRA, two types of event trees can be developed: functional and systematic. The functional event tree uses mitigating functions as it’s heading. The main purpose of the functional tree is to better understand the scenario of events at a high level following the occurrence of an initiating event. The functional tree also guides the PRA analyst in the development of a more detailed systemic event tree. The systemic event tree reflects the mitigative scenarios of specific events (specific human actions or mitigative system operations or failures) that lead to a hazardous outcome. That is, the functional event tree can be further decomposed to show specific hardware failure or human actions that perform the functions described in the functional event tree. Therefore, a systemic event tree fully delineates the process or system response to an initiating event and serves as the main tool for further analysis in the PRA.

The main elements of this step are:

1. Identify the mitigating functions for each initiating event (or group of events).
2. Identify the corresponding human actions, systems, software or hardware operations associated with each function, along with their necessary conditions for success.
3. Develop a functional event tree for each intiating event (or group of events).
4. Develop a systemic event tree for each initating event, delineating the success conditions, initiating event progression phenomena, and end effect of each scenario.

E) System Analysis

Event trees commonly involve branch point at which a given system (or event) either works)or happens) or does not work (or does not happen). Sometimes, failure of these systems (or events) is rare and there may not be an adequate record of observed failure events to provide a dependable data base of failure rates. In such cases, other system analysis methods such as reliability block diagram, fault tree analysis, and master logic diagrams may be used, depending on the accuracy desired. The most common method used in PRA to calculate the probability of system failure is fault tree analysis. This analysis involves developing a system model in which the system is decomposed into basic components or modules for which adequate data exist. Additional references about system techniques may be obtained from Modarres (1993), Kumamoto and Henley (1996), and PRA Procedures Guide (1982).

Different event-tree modeling approaches imply variations in the complexity of the system models that may be required. If only main functions or systems are included as event-tree headings, the fault trees become more complex and must model all dependencies among main and support systems (support systems provided services such as cooling, power, instrumentation and control, lubrication so that the main systems can properly operate). If support functions (or systems) are explicitly included as event-tree headings, more complex event trees but simpler fault tree will result.

PRA Calculation

The value in doing a PRA is not in the bottom line number that it produces, such as the reliability number or the probability of failure, but instead with its ability to *prioritize* risks based upon the model of the world and data inputs. There is typically a large uncertainty associated with both the model of the world and the data inputs, and to say that the number is a certain value detracts from the most useful benefits of the PRA analysis.

PRA codes take the model of events, event trees, scenarios and fault trees, and reduces it into its simplest Boolean form and determines the minimal cut sets. The minimal cut sets are the list of minimal basic event failure combinations that lead to system level failure. Based on probabilistic inputs, these minimal cut sets are prioritized from the largest contributor to the smallest. It is this prioritization that is most useful.

Example PRA Results

It is not the intent of this document to demonstrate how a PRA is to be done, but presenting example results can be helpful in discussing what managers can do with them. The list of cut sets below comes from a small PRA performed for a satellite experiment.

TABLE 4: Example Minimal Cut Sets From a PRA

Cut No.	% Total	% Cut Set	Frequency	Cut Sets
1	61.7	61.7	2.0E-2	Launch Vehicle Failure
2	71.3	9.6	3.1E-3	Spacecraft Power Failure
3	74.4	3.1	1.0E-3	Digital Subsystem Processing Failure
4	77.5	3.1	1.0E-3	Receiver Failure
5	80.6	3.1	1.0E-3	Digital Subsystem Timing Failure
6	83.6	3.1	1.0E-3	Upconverter Stable Local Operator Failure
7	86.7	3.1	1.0E-3	Upconverter Mixer Failure
8	89.8	3.1	1.0E-3	Upconverter Phase Lock Loop Electronics Failure
9	92.9	3.1	1.0E-3	Digital Subsystem Timing Failure
10	95.1	2.2	7.2E-4	Spacecraft Tilting Failure

These cut sets are for one end state, loss of mission. There could also be cut sets for loss of vehicle or other undesirable consequences, that all depends on the decision maker.

The first column is the cut set rank, e.g., first, second, third, etc. The second column is the cumulative total of the total failure probability. The third column is the percentage that single cut set is of the total. The fourth column is the frequency or probability of the cut set occurring. The last column is simply a description of the cut set or failure. This type of a description is much more helpful to the risk management process than just saying that the failure probability is a specific value.

Using PRA in Risk Management

By prioritizing the risks, PRA can be a very powerful risk management tool. By identifying the largest contributors to risk, a program manager can direct resources to areas that are most problematic. Cost-benefit analyses at this point will also help in determining which strategies will be most beneficial to the project. All of this is possible simply because the risks have been ranked.

For example, take the cut sets described in Table 4. Obviously the biggest risk to the mission is the spacecraft failing. If this risk is unacceptable, there may be a trade off between cost and using another launch vehicle with a higher reliability, although typically changing launch vehicles is difficult to do late in the project. If the risk of the power supply from the satellite is unacceptable, then perhaps a redesign may be desired for limited power capabilities. Similar risk reduction strategies can be conceived for all of the minimal cut sets, and the cost benefits of those can be estimated allowing management to make informed, risk reduction decisions at the programmatic level.

A PRA can be used to analyze a system at different levels and at anytime during the project. Although analyses done earlier in the design will often be at a higher level, there is still much insight that can be gained by doing the PRA. Typically, the sooner the risk drivers are identified, the cheaper they are to address. A PRA can easily pay for itself in terms of resources saved over the life of the program.

Basic PRA Characteristics

PRA is scenario based and works in failure space. It uses a string of events to diagram occurrences from an initial event or problem to an end result. Scenarios are developed typically using master logic diagrams (MLD's) to develop lists of events or loss of functions which could initiate failure scenarios, event sequence diagrams and event trees to represent the possible sequences of events, and fault trees which are useful in performing system analyses

Uncertainties and variabilities associated with the modeling of the physical and chemical aspects of events, the parameters of the models, and the frequency of events are explicitly identified by PRA. Bayesian analysis is used to combine information from analysis, databases, testing, and judgment. Monte Carlo simulation methods are used to propagate uncertainties and variabilities in the models at any level: fault tree, sequence or end state.

A PRA defines the damage levels and the frequency of obtaining each state using a system of algebraic equations. This is one major advantage of PRA: the ability to identify varying levels of degradation or success. Typically, reliability analyses focus at the extreme, it works or it doesn’t. Sometimes modeling the real world can be difficult with such a limited set of end states.

Scenarios in Risk Assessment

Scenarios are generally strings of events that lead to some kind of conclusion. The starting point for a scenario is called the initiating event. An initiating event is a problem or perturbation to the system that can cause an alteration in the normal operation. A scenario finishes with an end state or a damage state. An example of a damage state would be the loss of the Shuttle Orbiter. Damage states are defined by the decision-maker.

Between the initiating event and the damage state are pivotal events which determine whether the given damage state is reached as a result of the initiating event. Pivotal events may be protective (stop the failure at that point), mitigative (lesson the consequences), aggravative (make the consequences worse), or benign (basically no impact, but may be there for explanatory purposes).

Scenarios may be documented by a variety of different diagrams. In safety and reliability risk assessments the most common diagrams used are event trees, fault trees, and functional event sequence diagrams.

Master Logic Diagram

A master logic diagram is used to depict an arrangement of initiating events that is reasonably complete. It would be quite impractical to try to completely predict the occurrence of system perturbations in every detail. For this reason, analysts who wish to predict the relevant events use a functional categorization of perturbations to the system which lead to a component characterization of each function. The top event in a master logic diagram is the damage state, such as failure of an entire system. The lower levels of the diagram represent subsystem or component failures that lead to failure of the system.

It is important to note that in the classical sense, developed in the nuclear industry, a master logic diagram may have a different meaning than in other fields. For example, aerospace systems tend to be more dynamic and there may not be a set of initiators as such, but instead a list of events that need to occur. The set of events tress may instead be a single tree depicting an entire mission with the necessary functions being performed. There is no list of “initiators” in a case like this, just a list of events.

FESD's, Event Trees, and Fault Trees

Functional event sequence diagrams (FESD) are often used to present an outline of the system response to subsystem or component failures. An FESD is made up of an initiating event, pivotal events, and damage states. The pivotal events depict all the possible occurrences that could arise from the initiating event. An FESD is made using *inductive* reasoning, which means that consecutive events are developed by thinking of the next possible outcome. Each path in a FESD presents a different scenario.

An event tree, like an FESD is made up of binary outcomes for each event. Event trees are used because it is easier to obtain the needed algebraic equations than from a FESD, and most PRA programs use the event tree for quantification. Event trees require the probability of occurrence of each event. These probabilities may be developed using a fault tree or a singular event. In this way event trees and fault trees compliment each other. Together they depict the necessary and sufficient conditions for the occurrence of each damage state. As mentioned above they are used to find the needed algebraic equations.

A fault tree uses *deductive* reasoning, which means that the lower events are found by thinking of all possible ways in which the top event could have occurred. Using fault trees and event trees together is a more complete way of documenting scenarios than using either one individually. Although a single event tree or fault tree may be used to analyze simple systems, as the complexity of the system increases, using a single event or fault tree to model it rapidly increases in difficulty.

Uncertainties and Variabilities

Because probabilistic risk assessment is made up of very complex scenarios it is necessary to account for variations in physical processes and uncertainties in knowledge. Variability refers to changes in the physical process over the period of many similar trials. Uncertainty refers to knowledge of the parameter or variable.

Many variables and parameters could be determined without any uncertainty if sufficient experimentation could be performed. Unfortunately such experimentation is often unavailable if not impossible, and thus the uncertainty of a variable is represented not by a single point estimate, but by a stochastic distribution. Uncertainty will decrease as more knowledge of the parameters is made available. Uncertainties are developed at the lowest level of a risk model, such as the basic event level. PRA frameworks allow for appropriate treatment of variabilities and uncertainties.

Quantification of the uncertainties and variabilities is helpful in identifying the problems most important to risk. It tells us how confident we are with our results, and can be used in determining areas in which more testing is needed. It is an integral part of a PRA and should never be discounted.

4.0 Analyses Review Guidelines

Analysis review guidelines/checklists are provided in the respective analysis sections to assist the analysis reviewer and the originator. The assistance to the reviewer gives the minimum set of questions that need to be addressed in the review. The assistance to the analysis originator is not as directed and therefore is not as obvious. The assistance to the originator comes from the upfront knowledge of what the reviewer will be looking for in the analysis. Thus, the information can be provided in the initial documentation of the analysis rather than as a backfit during the review process.

4.1 General Review Guidelines

1. Does the configuration analyzed correspond to the flight configuration? If not, the originator should provide justification of the applicability of the analysis to the flight configuration within the analysis documentation package.

2. Is the basic data package, including the following elements, complete and adequately cited in the analyses?

   a) Circuit description

   b) Circuit drawing and revision designation

   c) Functional and logic block diagrams

   d) Functional and interface requirements

   e) Results summary and conclusions

4.2 FMECA

1. Single String Designs

   a) Was primary function protected by functional redundancy?

   b) Was verification made that loss of secondary function cannot cause loss of primary function?

   c) Was the analysis done to the piece-part level?

   d) Did the analysis include all appropriate mission modes?

2. Block Redundant Designs

   a) Was redundancy switching designed such that single failure in one branch does not propagate to the other redundant branch?

   b) Are inputs to redundant trains (i.e. power, signals, etc.) independent of each other?

c) Was a listing of all single failure points prepared?

4.3 WCA

1. Circuits

a) What functions were evaluated in the WCA?

b) What were the criteria for acceptable performance?

c) What functions were not analyzed and the justification for ignoring?

d) What were the design/analysis baseplate temperature limits that were used, and what was assumed for local part temperature rise above the base-plate temperature?

e) Was an analysis alternate such as Thermal/Voltage Margin test used?

f) Were voltage and/or frequency tolerances considered?

g) Was Extreme Value Analysis used or Root Sum of the Squares (RSS)?

h) Did parts parameter variations include initial part variation, aging (shelf life + mission), drift, special factors, radiation effects, etc?

2. Power Supply Analysis

a) Was transient performance considered, including current surges due to inrush and mode change?

b) Was the input filter reviewed for bus stability and ripple current reduction?

c) Were power consumption, power factor and DC component in AC loads considered?

d) Was overload protection (fuses and current limiters) considered?

e) Did grounding analysis consider external interactions and capacitive coupling of multiple grounds?

f) Were non-standard failure modes and the effects on power consumption, surges, ripple and power subsystem telemetry considered?

g) Were discrete semiconductors analyzed for peak transients on all terminals (i.e., collector, base, emitter, etc.)?

4.4 Part Stress Analysis

a) Were all parts analyzed?

b) What shearplate and junction temperature limits were used?'

c) What source (MIL-STD-975or other) was used for stress derating values?

4.5 Fault Tree Analysis

a) Was the top event consistent with specified functional requirements and broadly enough defined to include all top level functional requirements if there are more than one?

b) Is supporting documentation complete (i.e. system description, specifications, functional block diagrams, schematics, etc.) to verify that the hardware has been properly modeled?

c) Have all possible failure modes have been included in the fault tree branches?

d) Have the fault tree branches have been developed down to a hardware level for which there are well established failure modes. (Note: In some cases this may be the piece part level.)

e) Has that the companion FT prevention matrix has been developed and addresses the corrective action, design measure or product assurance activities that the project will implement to eliminate or minimize to the extent practical each of the identified failure modes?

4.6 SEE

a) What ambient and/or local environment was used?

b) What parts models were used?

c) What was the predicted upset rate?

d) Was an analysis of the impact of SEEs on system performance made?

e) Were there any unacceptable results predicted?

4.7 Parameter Trend Analysis

a) Were all key performance parameters selected for monitoring, by reviewing the functional performance requirements contained in the hardware specification and descriptive material on operation (see other analyses such as WCA, FTA, etc).

b) Do adequate monitor points exit for the selected parameters?

c) Has a well defined EOL criteria been defined both pre and post launch?

d) Has the prediction methodology been adequately defined mathematically for both the pre launch and post launch phases?

e) Is a periodic reporting process in place?

5.0 Analyses and Design Discrepancy Reports/Tracking System

5.1 General Discussion

Independent review of analyses is required on all projects. On a typical project there will be several hundred analyses generated and reviewed. The number of documents involved requires a computerized database to track the analyses and revisions and to periodically publish project-wide status reports.

The information to be tracked includes such items as:

1) Analysis ID number (memo, report, etc.)
2) Analysis type (PSA, WCA, FMEA, etc.)
3) Hardware to which analysis applies (assembly name, drawing and revision)
4) Analysis originator and organization
5) Analysis reviewer and organization
6) Release, revision, and review dates of analyses
7) Pass/Fail status of analyses
8) In process design changes

The above list is not intended to be all-inclusive, but only details the core content of the data base. The distinct output of each stage of the independent reviewer's assessment is documented in an Analysis Review Memo, and analyses that are deficient are reported in an "Analysis Discrepancy Memo" (ADM). The ADM and its contents are discussed in greater detail in Section 5.2.

The purpose of the design analysis is an assessment of the design adequacy of the hardware. The analysis may reveal an actual or potential problem with the hardware design or utilization. The extent of the issue can range from minor to catastrophic. Table 5-1 provides examples of several potential design discrepancies revealed by the various reliability analyses. All unresolved design issues are documented on a "Design Discrepancy Report" (DDR). The DDR and its contents are discussed in greater detail in Section 5.3.

A sample reliability analysis review process flow chart is provided in Figure 5-1

5.2 Analysis Discrepancy Memo (ADM)

The ADM is the independent reviewer's written documentation that:

1) Rejects deficient reliability analysis;

2) Describes the specific reasons for rejection (i.e. analysis methods are inadequate, significant errors are discovered, or documentation is incomplete and makes review impossible);

3) Lists the pertinent comments of the reviewer.

The ADM is identified by an "ADM" overstamp on the top of the reliability engineering office memo. Subsequent revisions to the ADM may be used to document acceptance of a revised analysis.

5.3 Design Discrepancy Report

Once all the analysis adequacy issues have been resolved, a thorough assessment of the hardware will be contained in the analysis package that represents the hardware. If the analysis or independent analysis review identifies an issue regarding the adequacy of the hardware design, a DDR will be issued.

If, the analysis reviewer discovers one or more discrepancies in the design, the relevant information on each such issue is rated as defined in Figure 5-2. This rating methodology is similar to the way Problem/Failure Reports (PFRs) are rated, but instead of utilizing understanding as a discriminator, the analysis issues are rated by the application or fix status. The definitions in Figure 5-2 are the criteria used to identify "Red Flag" issues. Once a "Red Flag" issue is identified, it is brought to the attention of the S/C Systems Manager for concurrence with the evaluation, and a Design Discrepancy Report (Figure 5-3) is prepared to insure the issues are adequately worked and formally brought off by a closed loop review process. An issue not considered red flag remains on the DDR summary until resolved. All red flag issues and unresolved non-red flag issues are reported to the project on this listing. In order to emphasize the significance of the red flag issues, a summary of these items is prepared (Figure 5-4).

5.4 Implementation Summary

This is to implement a process for focusing attention on significant design issues derived from the reliability analysis and provide tracking to their resolution. Figure 5-1 describes the process in a simple logic flow diagram. Required analyses are identified in the project reliability plans. An independent assessment of the analysis is performed by a reliability engineer and interacted with the appropriate JPL Cognizant Engineer or JPL technical manager. Analyses are then assigned status and tracked in a computer database. Periodically, summary status reports are published. Red flag issues are tracked until appropriate corrective action is implemented and the DDR is closed.

TABLE 5-1 Potential Design Discrepancies Revealed by Different Analyses

Analysis	**Potential Design Discrepancies**
FMECA and FTA	1. Revelation of previously unknown single failure points.
	2. Inability to switch between redundant hardware trains, given a certain initiating failure.
	3. The hardware does not possess the degree of fault tolerance (i.e. graceful degradation and/or partial survivability) required, given a certain initiating failure.
WCA	1. Hardware, namely electronic circuits, does not meet requirements under some combination of environmental, interface and/or end-of-life condition.
	2. Similar to above item, but discrepancy is associated with violation of some performance margin.
	3. Digital timing incompatibilities at key interfaces.
PSA	1. Piece part is found to be operating at too high a stress level (i.e. power, current, voltage or temperature) and violates established drating criteria. The high stress level, if uncorrected, would likely lead to premature failure of the overstressed part.
	2. Overstress due to unanticipated transient effects or erroneous assessment of duty cycle or specifications
SEE	1. Radiation sensitive piece parts.
	2. Intolerable upset rates.
	3. Latchup and/or hardware damage.
PTA	1. Premature aging of critical parameters

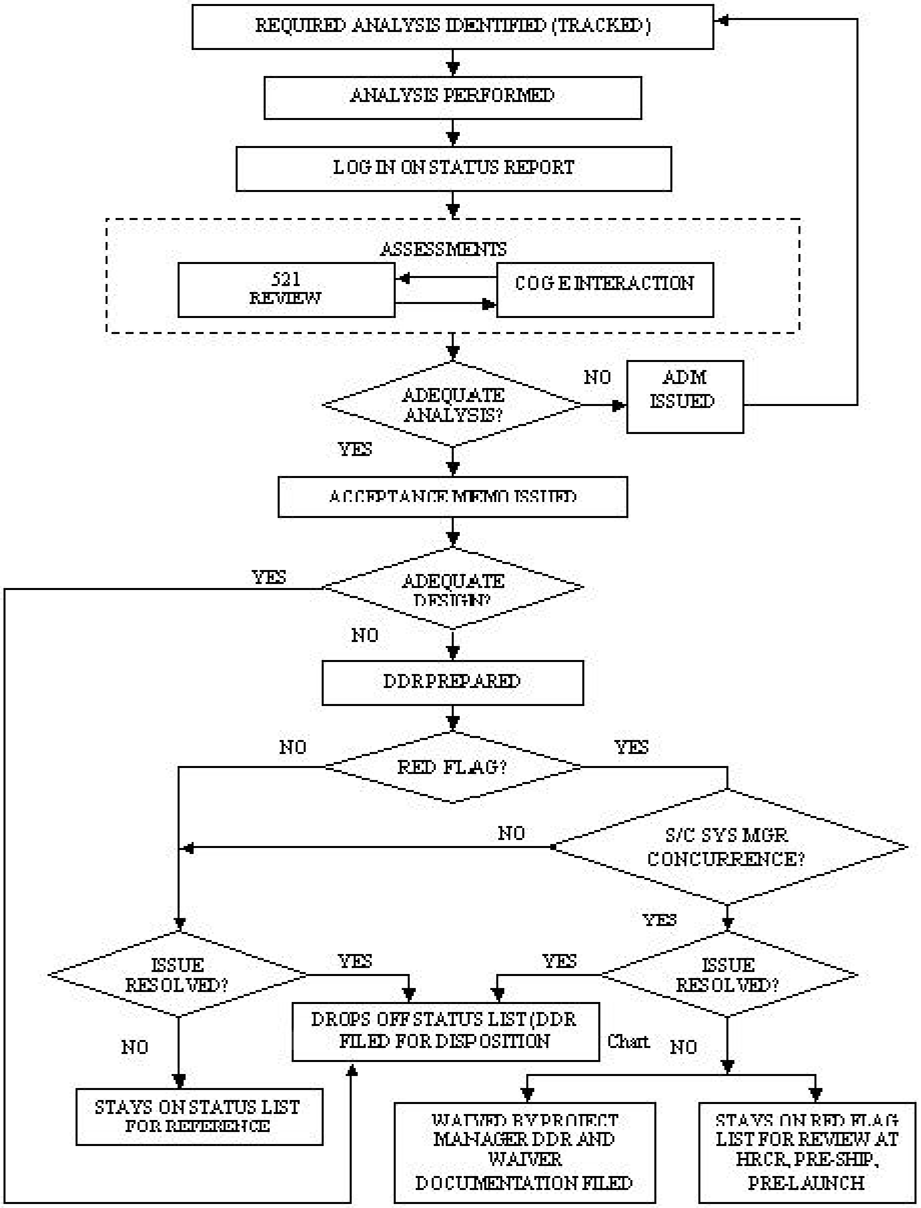


FIGURE 5-1 Analysis Review Process Flow Chart

METHOD OF SCORING AND RANKING DESIGN DISCREPANCIES

The categories of potential impact on mission success are:

1 = **Minor impact**. Can work around the problem should it occur or the effect is not significant.

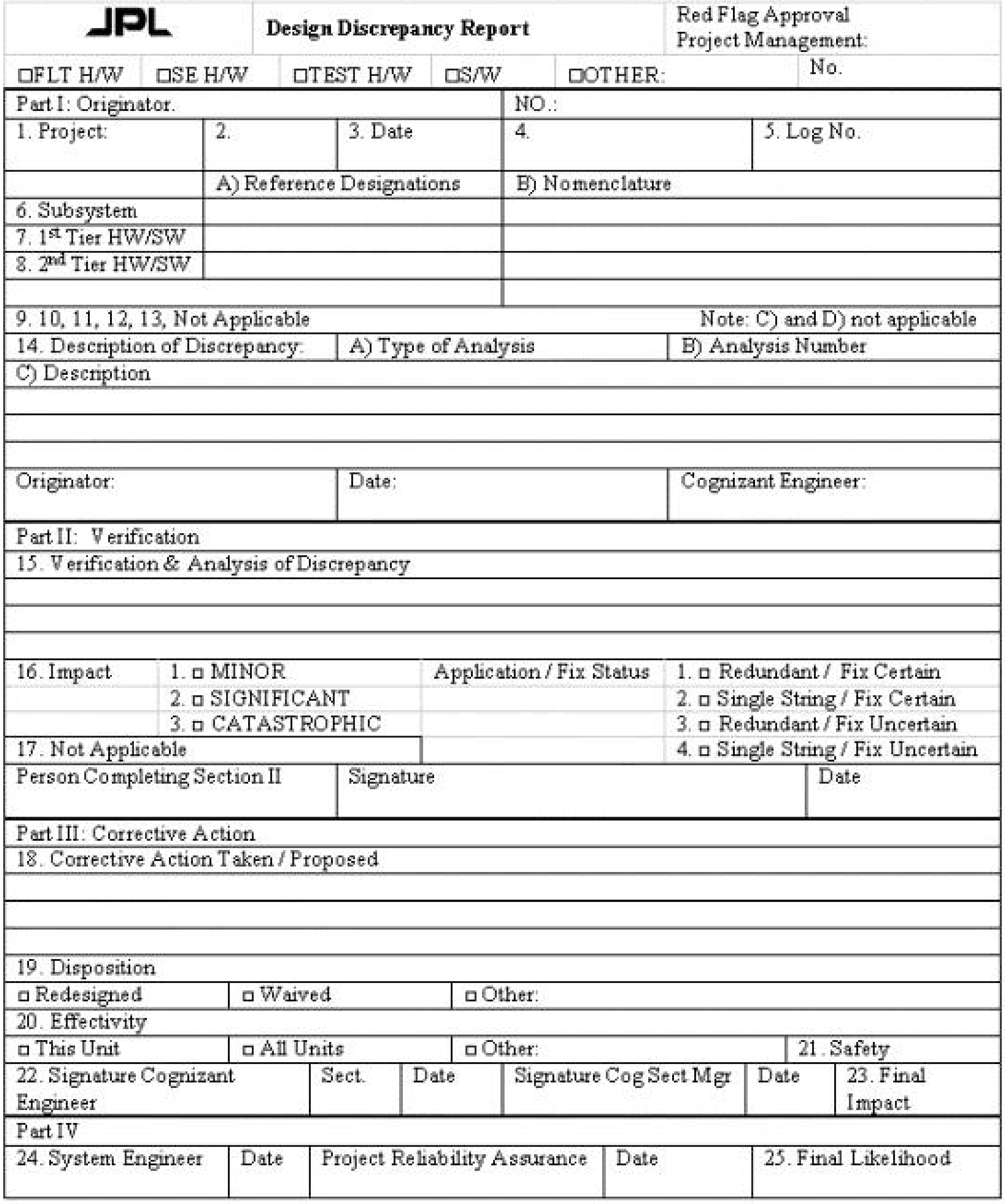
2= **Significant Impact**. Occurrence can have a significant effect on mission performance, but will not lead to loss of the mission.

3 = **Catastrophic Impact.** Occurrence can lead to loss of the mission or an unsafe condition.

IMPACT	SCORE		APPLICATION/FIX STATUS
Minor	1	1	Redundant circuit or Function/fix certain
Significant	2	2	Single string/fix certain
Catastrophic	3	3	Redundant circuit or function/fix uncertain
		4	Single string/fix uncertain

The scores inside the closed area are the Technical Red Flag definers (i.e, 2,3, 3,3 2,4 and 3,4 are defined as Technical Red Flag conditions).

FIGURE 5-2. DDR Ranking Criteria



JPL Design Discrepancy Report Red Flag Approval Project Management:

□FLT H/W □SE H/W □TEST H/W □S/W □OTHER: No.

Part I: Originator. NO.:

1. Project: 2. 3. Date 4. 5. Log No.

A) Reference Designations B) Nomenclature

6. Subsystem

7. 1st Tier HW/SW

8. 2nd Tier HW/SW

9. 10, 11, 12, 13, Not Applicable Note: C) and D) not applicable

14. Description of Discrepancy: A) Type of Analysis B) Analysis Number

C) Description

Originator: Date: Cognizant Engineer:

Part II: Verification

15. Verification & Analysis of Discrepancy

16. Impact 1. □ MINOR Application / Fix Status 1. □ Redundant / Fix Certain

2. □ SIGNIFICANT 2. □ Single String / Fix Certain

3. □ CATASTROPHIC 3. □ Redundant / Fix Uncertain

17. Not Applicable 4. □ Single String / Fix Uncertain

Person Completing Section II Signature Date

Part III: Corrective Action

18. Corrective Action Taken / Proposed

19. Disposition

□ Redesigned □ Waived □ Other:

20. Effectivity

□ This Unit □ All Units □ Other: 21. Safety

22. Signature Cognizant Engineer Sect. Date Signature Cog Sect Mgr Date 23. Final Impact

Part IV

24. System Engineer Date Project Reliability Assurance Date 25. Final Likelihood

FIGURE 5-3 Design Discrepancy Report

SUMMARY REPORT

DESIGN DISCREPANCY ISSUES

(DATE)

This report summarizes the concerns of JPL reliability engineering after reviewing the reliability analysis. The analyses concerns have been categorized as follows:

Impact	Score		Application/Fix Status
Minor Effect	1	1	Redundant Circuit or Function/Fix Certain
Significant	2	2	Single String/Fix Certain
Catastrophic	3	3	Red. Circuit or Function/Fix Uncertain
		4	Single String/Fix Uncertain

Dotted Area = Red Flag Design Discrepancy Reports

DDR CLASSIFICATION

There are 15 records with non-Red Flag risk/impact ratings. There are four (4) rating categories which comprise the Red Flag Reports divided as follows:

Impact, Application/Fix	DDRs
2, 3	1
2, 4	0
3, 3	1
3, 4	0
Sum	2

FIGURE 5-4 Example DDR Summary Report

Appendix A - Failure Modes Effects and Criticality Analysis (FMECA) Guidelines

1.0 Introduction

The purpose of the FMECA is to identify potential hardware design deficiencies and single-point failures. This design process is a systematic and documented analysis of the credible ways in which a system can fail, the causes for each failure mode, and the effects of each failure. The objective of the FMECA is to identify all single function failures and their effect on performance in order to validate redundancy or partial survival capability. Furthermore, it verifies that lower level failures do not propagate within the spacecraft. The FMECA is a prime analytic method to guide design and system trade-off study.

A FMECA will be performed at the functional block level. In addition, a piece-part FMECA is required at all unit-to-unit interface circuits to preclude any propagation of irreversible hardware failures. A piece part FMECA is also required on the support equipment-to-flight equipment interface circuits to preclude the propagation of support equipment failures into the flight units (assemblies).

It is important that connectors, harness, and internal wiring failures be included in the FMECA for those connections which have not been verified prior to launch (by successful subsystem or system testing and remaining mated). See Section 7.0 of this Appendix.

2.0 Steps In Performing FMECA

There are six essential steps in the performance of an FMECA:

(1) Reliability block diagram construction: A reliability block diagram is constructed indicating the functional dependencies among the various elements of the system. The detail should be down to the part level at interfaces between units.

(2) Failure definition: Rigorous failure definitions must be established for the system, subsystem, and all lower equipment levels. As a minimum, the part failure modes to be assumed are given in Table A-1.

(3) Failure effect analysis: A failure effect analysis is performed on each item in the reliability block diagram. This takes into account each different failure mode of the item and indicates the effect of that item's failure upon the performance of the next higher level in the block diagram.

(4) Bookkeeping task: The system and each sub-item must be properly identified and indexed.

(5) Critical items list: The critical items list is generated or updated based on the findings in steps 1, 2, and 3.

Table A-1. Minimum Part Failure Mode Assumptions

Part	**Failure Modes**
Capacitors	Short Circuit; Excessive leakage (electrolytic); Open circuit
Circuit breakers	Failed open; Failed closed
Coils	Open winding
Connectors	Shorts (pin to pin), see paragraph 7.0; Shorts (pin to ground.); Opens (pin to pin)
Diodes	Short circuits; Open circuits
Insulators	Electrical breakdown
Microcircuits (outputs only, digital and analog)	Saturated High; Saturated Low; Open (Hi Z output)
Microprocessors	
Functional	TBD
Output lines	Same as microcircuits
Relays - electromechanical	Contact permanently closed; Contact permanently open;
	Excessive contact bounce
Resistors	Open circuit
Switches, rotary	High resistance contact; Open/Short
Switches, toggle	Permanently open; Permanently closed
Transformers	Shorted turns; Open circuits
Transistors - bipolar	Shorted CE; Shorted CB; Open circuit C, B, or E
Transistors - FET	Shorted DS; Shorted GS; Open circuit G,D, or S

(6) Documentation task: Define the baseline design configuration and operation. List the FMECA assumptions. Attach completed FMECA worksheets, and (See Figure B1) supporting diagrams, drawings and analyses.

3.0 Identification of Critical Failure Item

Based on the failure effects analysis, a list of critical items is prepared. This list contains those items whose failure can result in a possible loss, probable loss, or certain loss of the next higher level in the reliability block diagram. All items that can cause system loss should be identified clearly by their inclusion in the critical items list.

4.0 Single Point Failure Identification

Critical failures must also be identified in accordance with D-8061 paragraph 3.2.1 "JPL Standard for Reliability Assurance".

5.0 Redundant Block FMECA

Subsystems incorporating block redundancy must be subjected to a FMECA at the piece part level for all subsystem interface circuits between the redundant blocks and the sensing/switching circuits. This piece part FMECA is done to verify redundancy and partial survival capability for blocks with redundancy.

6.0 Interlocking System Level FMECA

Multiple FMECAs are required to carry the chain of failure effects from the lowest level failure sources to the spacecraft level for some complex subsystems. The determination of a single point failure (SPF) at the spacecraft level may require an analysis of effects beyond the interface of the subsystem or system generating the failure and its effects. Multiple system effects may be generated directly from the single initial failure, some of which may result in a SPF in another system. The Fault Detection System (FDS) may prevent a SPF in a way not evident to a subsystem designer generating a lower level FMECA.

An interlocking higher level FMECA will be provided when a lower level FMECA is determined to lack sufficient visibility into the criticality of failure effects at the spacecraft level. The overlap between the lower level and higher level FMECAs should be adequate to allow analysts working at either level to communicate effectively (equipment to spacecraft and in the reverse direction). Clear understanding of the cause and effect relationships of failures that can cause SPFs must be documented.

The inability of a lower level FMECA to clearly resolve a SPF effect by the Preliminary Design Review (PDR) should immediately trigger a request for the generation of a higher level FMECA to define the SPF potential of the design in question.

The higher level FMECA (usually to the spacecraft level) should reference the lower level FMECA reviewed at the PDR. Additional failure modes arising at the PDR and design concerns resulting from the PDR are additional inputs besides the lower level FMECA at the start of the spacecraft level FMECA.

7.0 Connector, Cable And Insulator Failures

Because of the relatively benign nature of the mechanical and physical environments of a spacecraft, certain simplifying assumptions can be made relative to connector and cable failure FMECAs. These assumptions are based on the following facts:

A. The unit (box) and spacecraft design integrity of conductors and insulators has been verified by the flight qualification or protoflight test process.

B. Any multiple units are built and inspected to the same drawings and manufacturing processes as the qualified units.

C. The mating of all required harness interconnects is considered validated provided they have been exercised by an appropriate subsystem or system test and have not been de-mated since the test.

Those connectors for which FMECAs (bent pin analysis) are required are as follows:

1. Connectors which were not verified for mating by a subsequent subsystem or system level test (umbilicals, pyros, etc.).

2. Connectors for which mismating could result in serious personal injury or hardware damage upon initial mating (i.e. to energy sources or powered mechanisms).

3. Connectors which are part of a cable assembly which experiences multiple (greater than ten) flexings as a part of its normal operation (unless twice the full mission flex life has been demonstrated by test).

In these three (3) cases, all physically realizable pin to pin and pin to shell shorts, as well as opens, must be considered by the FMECA.

8.0 FMECA Example

Many treatments of failure mode, effects, and criticality analysis (FMECA) methodology have been developed and any rigorous treatment is acceptable. Figure A-1 is an example of a portion of a FMECA.

Identify and list the individual functions from a functional block diagram of the hardware to be analyzed. Break the system down to the lowest level functional hardware blocks. The composition of each block will be determined by the type of system being analyzed. It is not the intent to reduce block detail to the individual part level. It is intended that the hardware be broken down to those functions which are essential to the task for which the hardware was designed. For example, power circuits are designed to deliver voltage and current. The functions involved in this task are usually source isolation, rectification, voltage multiplication, filtering, feedback regulation, over-voltage protection, and current limiting. All redundant or repetitive blocks should not be so complex that they encompass multiple internal functions.

Draw the block diagram with all the internal interconnections. Label the blocks and connections with sufficient detail for positive identification with schematics and other identified design sources. All external functions, command inputs, loads, and environments should also be analyzed if sufficient knowledge is available. Otherwise they must be described to the fullest extent possible.

If a block critical to the hardware performance has an excessive number of failure modes, it is a candidate for further study (FMECA at the piece-part level or other appropriate technique).

The details of required data for each column of the FMECA worksheet (Figure A-2) are defined below:

(1) Item. Name of the item under analysis. The system under analysis shall be divided into the lowest level of description practical. Include the drawing number of the reference designator by which the contractor/manufacturer identifies and describes each item or standard grouping of items.

(2) Mission phase. If appropriate, identify the mission phase(s) for which an item failure mode is being investigated (i.e., ground check, prelaunch, attitude stabilization, cruise, midcourse maneuver, final man-maneuver, orbit).

(3) Failure mode. Describe the specific failure mode, considering (as a minimum):

(a) Premature operation.

(b) Failure to operate at a prescribed time.

(c) Failure to cease operation at a prescribed time.

(d) Failure during the prescribed operating period (nonstandard operation). Typical failure modes are: no output, rupture, drift, excess noise, etc.

(4) Most Probable Failure Cause. Describe the mechanism which has the highest probability of inducing the failure. This entry establishes the credibility of the failure mode.

(5) Failure Effect. Describe the effect of the item failure mode on:

(a) System.

(b) Interfaces.

(c) Other items.

(d) Mission.

(6) Criticality and Probability. Describe and rank the criticality of the function from 1 to 6 with 6 being most critical to the mission success as defined below:

6 - complete loss of mission: complete loss of primary mission capability.

5 - major loss or degradation of mission: capability to complete some mission objectives (or all at a degraded level) with immediate loss of a critical science instrument or loss of a major amount of critical science data, or major reduction in life of mission, or loss of spacecraft function resulting in loss of opportunity for obtaining critical science data.

4 - significant loss or degradation of mission: significant loss of spacecraft or instrument function leading to a significant loss of data, or a significant reduction in life of the mission.

3 - loss or degradation of a redundant subsystem: loss or degradation of a subsystem or science instrument producing levels 6, 5, or 4 criticality, if remaining redundancy is lost.

2 - potential for major or significant degradation of spacecraft or performance: no immediate impact on spacecraft or mission, but potential exists for future loss, at level 6-3, due to induced failure, or resulting from the conjunction of this anomaly with a future event, or potential for cumulative major loss of function over a long period of time; or major or significant degradation of mission, at levels 6-3, would have occurred if adequate alternatives or measures had not been implemented.

1 - minor or no impact on spacecraft life or performance: noticeable or no degradation, but does not lead to instrument loss, or loss of significant amount of data, or significant reduction in quality of data, or significant peril to mission.

Determine whether the probability of the failure occurring is high, low, or medium.

(7) SPF – Identify if a Single Point Failure to the Mission (mission terminated). If unable to define at this level of analysis attach a document requesting a determination from the project office.

(8) Failure Mode Detection - Identify the indicators by which a particular failure mode is detected (test, inspection, or TLM), and list specific tests or monitor points, as well as a qualitative assessment of the indication.

(9) Remarks - List appropriate remarks with respect to each failure mode.

9.0 FMECA Review Checklist

The following analysis review checklist is provided to assist the analysis reviewer and the originator.

1. Single String Design

   a) Was primary function protected by functional redundancy?

   b) Was verification made that loss of secondary function cannot cause loss of primary function?

   c) Was the analyses done to the piece-part level?

d) Did the analysis include all appropriate mission modes?

2. Block Redundant Designs

a) Was redundancy switching designed such that single failure in one branch does not propagate to the other redundant branch?

b) Are inputs to redundant trains (i.e. power, signals, etc.) independent of each other?

c) Was a listing of all single failure points prepared?

3. Mechanisms

a) Was FMECA or Fault Tree Analysis performed to the lowest level of disassembly?

b) Were mechanisms tested/analyzed to control failures?

Item	Mission Phase	Failure Mode	Most Probable Cause	Failure Effect		Probability/Criticality to Mission	Failure Mode Detection	Remarks
				Subsystem	System			
Battery	Boost	Shorted Cell	(a) Breakdown of cell separator	Reduced Battery Voltage	Less power available, might limit mission success	Medium to high/medium	Low flight T/M voltage	Proper separator selection, plate/ cell Fab & QC should reduce probability
			(b) Metal particle in cell					Monitor cells for loose particles during vibration test
		Open cell	(a) Broken cell inter-connects	Battery voltage becomes zero	Removes battery from S/C system	High/High	Flight T/M voltage goes to zero	Redundancy would greatly reduce probability
			(b) Broken case- eletrolyte leakage	(1) Reduced cell voltage	(1) Reduced power available	(1) Medium during leaking, high/ medium when dry	Flight T/M voltage decreases	Vibration test should verify case design
				(2) Could damage adjacent hardware	(2) Could short open electrical circuits	(2) High/high		

Figure A-1. Example of a Part of a FMECA

<table>
<tr><td colspan="4">Figure A-1. FMECA Example</td><td colspan="3"></td><td colspan="3">Date:</td></tr>
<tr><td colspan="10">Failure Modes, Effects, Criticality, and Analysis</td></tr>
<tr><td colspan="4">Analyst:
Indenture Level:</td><td colspan="3">Assembly Name:</td><td colspan="3">Schematic No.
Location:</td></tr>
<tr><td rowspan="2">Item</td><td rowspan="2">Mission Phase</td><td rowspan="2">Failure Mode</td><td rowspan="2">Most Probable Cause</td><td colspan="2">Failure Effect</td><td rowspan="2">Probability/Criticality to Mission</td><td rowspan="2">Failure Mode Detection</td><td rowspan="2">Remarks</td><td></td></tr>
<tr><td>Subsystem</td><td>System</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure A-2. FMECA Worksheet

Appendix B - Worst-case Analysis Guidelines – Circuit And Power Supply

1.0 Purpose and Scope

This document is intended to guide the Cognizant Engineer or his designated analyst in the performance and/or review of a worst-case analysis. This analysis is usually required of all electronic assemblies.

2.0 Applicable Documents

D-XXXX	Project Specific Environmental Requirements Document
JPL D-10133	Calculation of Part Parameter Variations (WCA)
NASA et all	Radiation Effects Electronic Data Bases (Refer to appendix G; paragraph 5.6)

3.0 Requirements

3.1 True Worst-case Analysis

The analysis will be true worst-case in that the value for each of the variable part parameters will be set to limits which will drive the output(s) to a maximum or minimum or both, depending on the circuit function. Consideration shall be given to AC, DC, and transient effects on the circuit being analyzed. Circuits consisting of interconnected digital IC's of a singular technology (e.g. all LSTTL, all CMOS, etc.) will be subject to worst-case analysis for timing and capacitive load considerations and possible "race" conditions. Mixed digital technologies also require interface compatibility analyses.

One of the most important elements in the WCA is the part parameter variations used for the piece parts in solving the circuit equations. If a design is to pass a WCA, it must be designed with the same worst-case part parameter variations to which it will be subjected in the WCA. Tables B-1 through B-8 serve as a guide for part parametric variations to be used in the performance of the worst-case analysis.

3.2 Procedural Considerations

To facilitate the performance of the WCA, the analyst may reduce complex circuits to smaller functional blocks. By using this approach the analysis becomes more manageable, so both the analyst and the reviewer are aided. When a circuit is reduced to these functional blocks, performance requirements for each block need to be established. Both input and output requirements should be established. These requirements will serve as the evaluation criteria for the WCA results for the functional blocks. If such criteria exist in another document (e.g., design verification requirements document), reference to the source document should be made. Some of the requirements for the functional blocks must be derived from higher level specification requirements. In this case, the method of deriving these requirements shall be clearly shown.

The WCA report should show compliance with all requirements, both on the functional block level and at the circuit level. Deviations from these requirements are to be noted explicitly and any proposed solutions outlined as part of the report. Proof of compliance to certain less significant requirements may be omitted provided that adequate justification for the specific omission is given in the WCA analysis report. It is recommended that the assumptions and approach to be used in the analyses be concurred with by the project Reliability Engineer prior to the performance of the analyses.

To simplify the discussion, the remainder of this guideline will refer to circuits, but is intended to apply to the lower level functional blocks also. If design changes are made, either as a result of the WCA or for other reasons, the WCA report is to be updated using the new circuit.

The temperature over which the part parameter variation database is defined is tied to the environmental design requirements for a specific mission. Figure B-1 shows the various temperature definitions / requirement for a typical project:

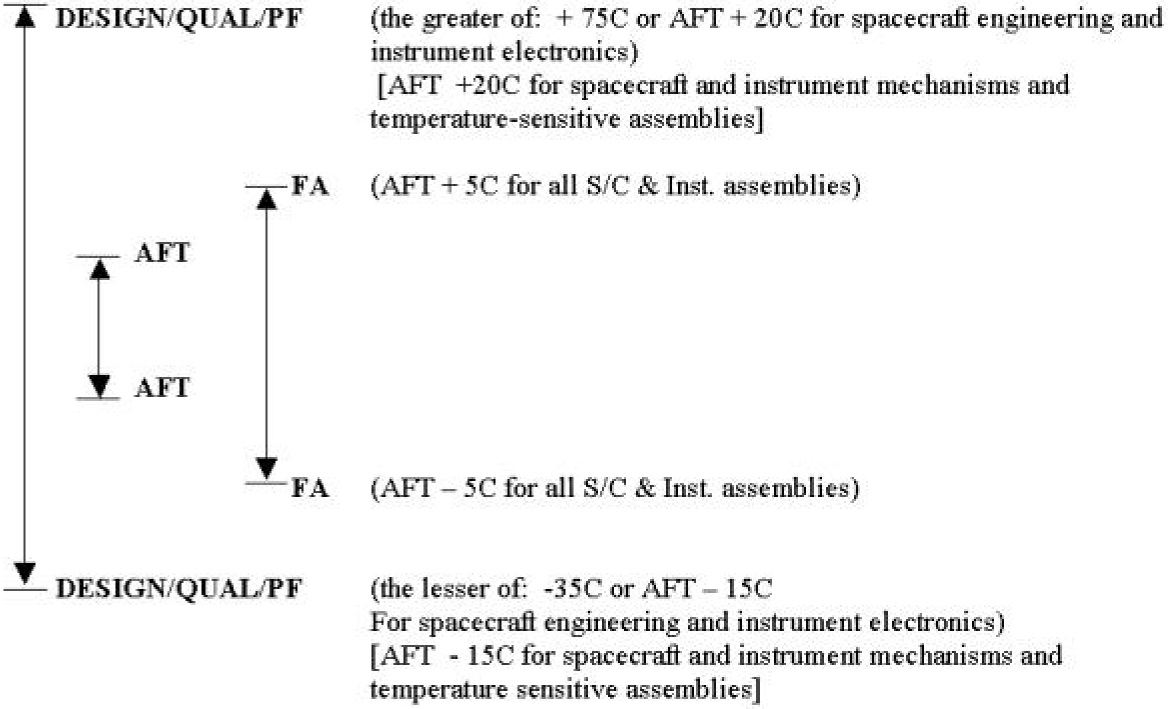

DESIGN/QUAL/PF
(the greater of: + 75C or AFT + 20C for spacecraft engineering and instrument electronics)
[AFT +20C for spacecraft and instrument mechanisms and temperature-sensitive assemblies]
FA
(AFT + 5C for all S/C & Inst. assemblies)
AFT
AFT
FA
(AFT – 5C for all S/C & Inst. assemblies)
DESIGN/QUAL/PF
(the lesser of: -35C or AFT – 15C
For spacecraft engineering and instrument electronics)
[AFT - 15C for spacecraft and instrument mechanisms and temperature sensitive assemblies]

Figure B-1

Notes:

1) The above definitions/requirements will be defined at the thermal control surface of each assembly for each given project. Part body temperature extremes assumed in the part data base must be verified using the detailed thermal analyses of each assembly. WCA serves as analytical verification that functional specifications have been met over the protoflight/ qual temperature range.

2) The definitions applied to Figure 3-1 are given on the next page.

Temperature Definitions

Operating Allowable Flight Temperature

Operating Allowable Flight Temperatures (AFT) are the mission temperature limits (including allowance for prediction uncertainties) in a worst-case powered-on operational (operating within functional specifications) mode that the thermal control is designed to maintain for specified assemblies and subsystems (hot or cold). All temperatures are measured at the thermal control surface (e.g. mounting surface, radiator surface, etc.), as specified by Thermal Engineering.

Non-Operating Allowable Flight Temperature

Non-operating Allowable Flight Temperatures (AFT) are the mission temperature limits (including allowance for prediction uncertainties) in a worst-case powered-off, non-operational mode that the thermal control is designed to maintain for specified assemblies and subsystems (hot or cold). Unless otherwise specified, assemblies are required to start up from a non-powered state within the Non-op. AFT and operate within functional specifications once within the operating AFT range.

Design Temperature Limits

Temperature limits to which assemblies are designed to meet functional and performance specifications; normally equivalent to the Qualification/Protoflight limits.

Qualification Tests

Qualification tests are formal environmental tests performed on a dedicated Qualification Model or flight-like Engineering Model of flight hardware which is not intended to fly in order to demonstrate flight design adequacy and quality workmanship. Thermal environmental qualification testing is equal to Protoflight level testing. Dynamics environmental testing is equal to Protoflight level testing in magnitude and exceeds it in duration. Qualification implies meeting all functional specifications in the operating environments.

Qualification by Similarity

May be defined as the procedure of comparing an item which has not undergone Qualification testing to another item having only minor differences in configuration and functional characteristics which has been:

1. Tested to stress levels at least as severe as those specified for the item to be qualified;
2. Tested under equivalent program controls;
3. Manufactured by the same supplier using similar application.

The item also may be identical to one previously qualified and successfully flown.

Protoflight Tests

Protoflight (PF) testing is performed on flight hardware, which is intended to be flown and having no previous qualification test article. Protoflight testing accomplishes in one test the combined purposes of design qualification and flight acceptance.

Protoflight thermal test levels and durations are identical to qualification test levels and durations. Protoflight dynamics test levels are equivalent to qualification test levels; however, the duration is lowered to flight acceptance duration. PF testing includes meeting functional specifications under protoflight environments

Flight Acceptance Tests

Flight Acceptance (FA) environmental tests are typically performed on flight hardware and spares to verify flight workmanship quality, but only when a previous protoflight or qualification test has been performed on an identical item to qualify the design. FA test levels may also be used to verify the quality of reworked flight hardware. FA testing includes meeting functional specifications under flight acceptance environments.

Flight Acceptance testing should be evaluated for use on a case-by-case basis. If it is determined by a Heritage Review that previous qualification or protoflight test levels on a heritage assembly envelope those required for the new assembly and the heritage design, and operation is not modified in such a way as to negate the previous qualification, then the assembly may be Flight Acceptance tested.

3.3 Worst-case Conditions

The worst-case conditions of any given circuit will be a combination of the extreme values of the following factors:

1. Circuit Interface Inputs and Loads
2. Piece Part Parameter Variations

These factors are described in the following paragraphs.

EVA (Extreme Value Analysis) is the primary approach for both the derivation of part variations and the combinations of circuit part values, it yields very conservative results which represent very improbable conditions. When this process yields unacceptable results, the design/analyst may perform a statistical WCA at some pre-agreed level (usually 3 sigma). These analyses can be accomplished using either RSS'd or Monte Carlo analyses for both (or either) part variations and circuit variations.

The RSS process does not simply RSS every variation. Biases in parameters (such as temperature and radiation effects) must remain as biases and algebraically added to those variations which are truly random (i.e. in-determinant in direction and uncorrelated to other variations).

3.3.1 Circuit Interface Inputs and Loads

The inputs to the circuit shall be taken to their maximum and minimum voltage and frequency, with the intention of driving the outputs of the circuit to their maxima and minima. The variation of signals presented to the circuit being analyzed are to be those continuous values which are applied at the inputs to the circuit. If the circuit is a control circuit which feeds back, in effect, to its own input (e.g., a regulator circuit), it is to be subject to the limits of its control range in the WCA.

Likewise the interface characteristics on the circuit's output side must also be taken to the appropriate maximum or minimum extreme, and its input stimulus must span the limits of its specified variations.

3.3.2 Piece Part Parameter Variation

The total parameter variation depends on variations resulting from a number of causes. The EVA (Extreme Value Analysis) worst-case variation for any one part-parameter is the product of the individual parametric variations as follows:

$(1+dP) = (1+dX)(l+dS)(l+dT)(l+dE)(l+dR)$ B-3

where: dP is the total parametric variation

dX is the part initial tolerance

dS is the variation due to aging and drift

dT is the variation due to temperature (worst-case direction) dE is the variation due to applied voltage and frequency

dR is the variation due to radiation degradation

All of the above deltas are normalized as variations from their nominal; that is a +1% initial tolerance yields a dX of 0.01.

If the selected device is sensitive to mechanical or other factors, such as impact, stress, vibration, vacuum, etc., that sensitivity must be included in the WCA.

As noted above, the equation yields an EVA solution for part variations. For a project statistical approach to part variations, the sources of variation must be separated into their biased portions (i.e. predictable in direction) and their random portions (i.e. not predictable in direction). The random contributors can be RSS'd and added to the biases to yield a statistical worst-case.

The above variations are described further in the following paragraphs.

3.3.2.1 Piece Part Initial Tolerance.

The tolerances to which a manufacturer has screened the devices shall also be accounted for. There is no additional tolerance to be added to that specified by the manufacturer. Parts whose tolerances are the same cannot be assumed to track in temperature or time in the WCA.

3.3.2.2 Part Aging and Drift (End-of-Life Factors).

The aging of electronic parts is a continuing process of chemical change. In most cases, the rate of chemical change is an exponential function of absolute temperature and decreases exponentially with time. This temperature and time dependence provides a means of predicting life expectancy. For the purposes of WCA, life is considered ended when a part parameter drifts outside the circuit allowable limit for that part.

3.3.2.3 Temperature Levels.

The upper temperature extreme to which parts at the AFT limits to be analyzed shall be based on a thermal analysis of a shearplate at the AFT limits which predicts the operating temperature rise between the shearplate and the part. The lower analysis temperature extreme shall be the lower AFT with no rise assumed.

3.3.2.4 Applied Voltage and Frequency.

The parameter variation resulting from the applied voltage and frequency must be included. For example, the effective capacitance of a capacitor is a function of both the applied voltage and frequency.

3.3.2.5 Effects of Radiation.

Most passive components are not subject to degradation at typical space exposures of total dose radiation levels. Semiconductors, however, are susceptible to degradation due to radiation. The most current data are contained in the continually upgraded electronic data-bases in appendix G; paragraph. 5.6.

3.4 Verification By Test

In some cases, (e.g., RF circuitry) the modeling and analysis of a circuit may prove to be extremely difficult and questionable for certain parameters. In these cases, it may be expedient to use laboratory test data in conjunction with analysis to determine the worst-case response. For those parts that are difficult to model, the laboratory test is used to establish the sensitivity which can be used in a simplified analysis to achieve all worst-case conditions, accounting for each of the six factors mentioned above. This approach will require careful selection of the devices installed in the circuit to achieve the desired shift from nominal part values, either by selection of outlier parts or parts intentionally degraded prior to testing. This sensitivity is used to scale circuit performance for the defined worst-case part variation. The remaining parts are evaluated by standard WCA analytical methods.

3.5 Analysis

This section provides general guidelines for performing the WCA. More detailed guidelines, for specific circuit types, are provided in Section 5.0 of this appendix.

3.5.1 Analytic Preparation

In order to expedite the WCA, the parameters which affect the individual component's operation must be delineated prior to any attempt at circuit simulation or evaluation in the WCA. Tables 1 through 8 of this appendix address part parameter variability. The parameter variations include the effects described in paragraph 3.3.2.

3.5.2 Computer Aided Analysis

The WCA can be simplified by doing a computer aided analysis. The availability of WCA tools simplifies the analysis by relieving the analyst of the need to explain his personal methods as part of the WCA and standardizes the analysis methodology. The use of computer aided analytic tools is encouraged. The proper application of these tools requires that the analyst understand the device models used by the programs and must use the true worst-case approach with the programs. If these tools are used, the analyst must include a description of the circuit models used and a summary of the analyses performed. Summary printouts should be included with the WCA report as an appendix.

3.5.3 Sensitivity Analysis

The worst-case maximum or worst-case minimum or both are required, depending on the circuit function, and the use of circuit simulation software will simplify the performance of the WCA. The ideal program uses a sensitivity analysis to automatically select the worst-case combination of parts parameters. Other programs provide the sensitivity analysis only, so the analyst has to enter the sign and magnitude of the part variations into the network analysis program. The sensitivity of an output parameter 'y' to a part variable 'x' is the expected change in 'y' per unit change in 'x'. If the sensitivity of parameter y to parameter x is 0.5, a 4% change in 'x' results in a 2% change in 'y'. Digital computers handle the required matrix manipulations easily.

3.6 Results

After the worst-case computations have been completed, the results must be documented. Any results which show the circuitry operating beyond specified limits are to be noted. The analysis should provide adequate information to permit the necessary programmatic trades of either a modified analysis technique, redesign, or special testing. The analyst should be prepared to appropriately support the resultant actions. A flow diagram of the generation and approval of the WCA is shown in Figure B-2.

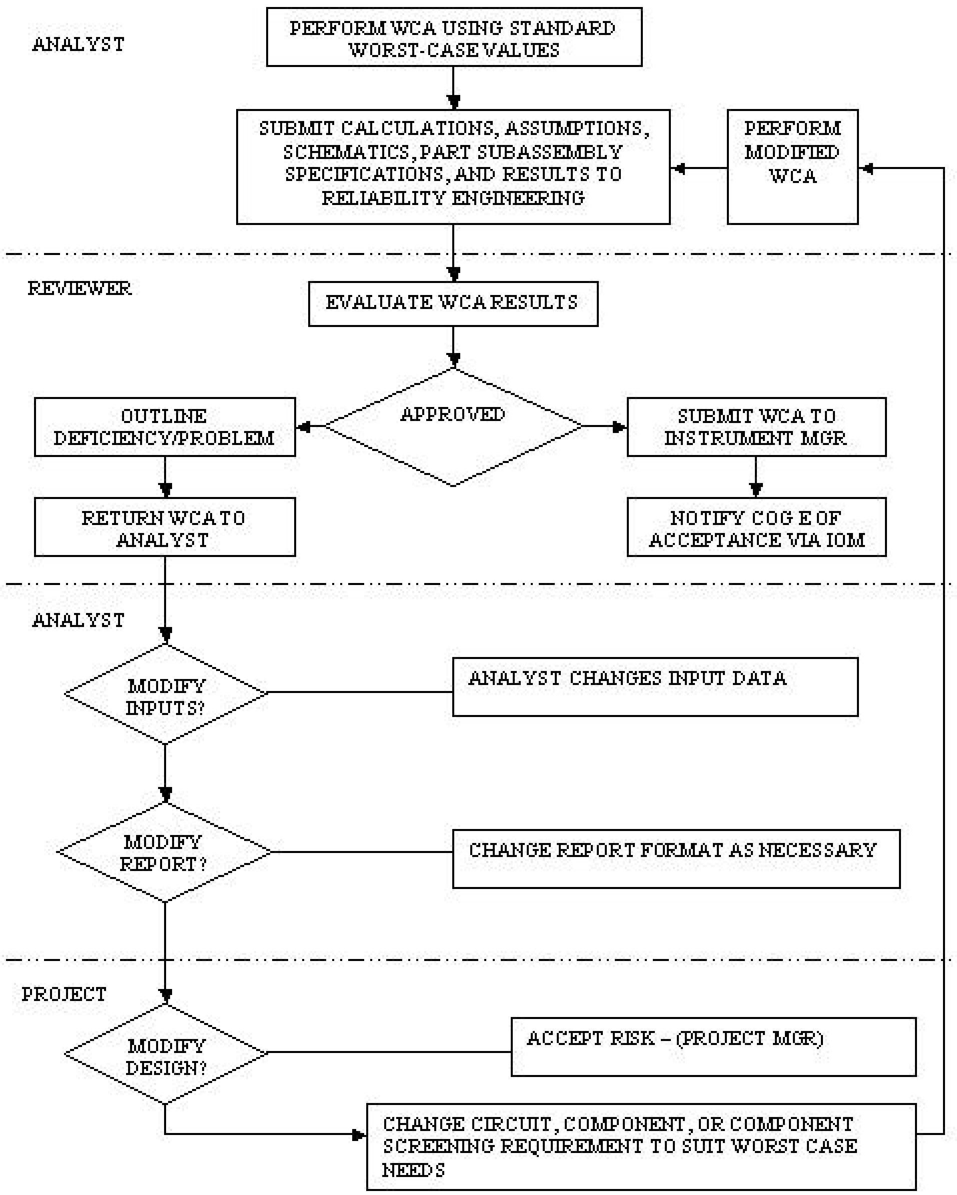

ANALYST
PERFORM WCA USING STANDARD WORST-CASE VALUES
SUBMIT CALCULATIONS, ASSUMPTIONS, SCHEMATICS, PART SUBASSEMBLY SPECIFICATIONS, AND RESULTS TO RELIABILITY ENGINEERING
PERFORM MODIFIED WCA
REVIEWER
EVALUATE WCA RESULTS
APPROVED
OUTLINE DEFICIENCY/PROBLEM
SUBMIT WCA TO INSTRUMENT MGR
RETURN WCA TO ANALYST
NOTIFY COG E OF ACCEPTANCE VIA IOM
ANALYST
MODIFY INPUTS?
ANALYST CHANGES INPUT DATA
MODIFY REPORT?
CHANGE REPORT FORMAT AS NECESSARY
PROJECT
MODIFY DESIGN?
ACCEPT RISK – (PROJECT MGR)
CHANGE CIRCUIT, COMPONENT, OR COMPONENT SCREENING REQUIREMENT TO SUIT WORST CASE NEEDS

Figure B-2 Generation and Approval of the WCA

4.0 Report Format and Content

General documentation requirements are discussed in Section 2.0 of this document. The report should also contain the following specific information.

4.1 Title Page

The title page shall give the project name and number, the system/subsystem/assembly and circuit names, the analyst's name and the date on which the analysis was performed.

4.2 Applicable Documents

All documents, which contain requirements to which the circuit is to conform, should be identified. The circuit schematic number and revision code should also be identified. The circuit schematic number and revision code should also be listed. A copy of the schematic should be included with the WCA report.

4.3 Circuit Description

The circuit function should be clearly explained relative to any circuits with which it interfaces. In addition, the theory of operation of the circuit should be discussed in this section in plain language, avoiding numerical values and circuit specific facts as much as possible.

4.4 Performance Requirements

The specified and derived requirements for the circuit, which form the analysis acceptance criteria, should be listed in matrix form. The matrix should show the parameters on one axis, the source of the requirement on the other axis, and the actual specified value at the intersection of row and column. The source of all acceptance criteria should be referenced to documents listed in section 4.2 of this report.

4.5 Analysis

The analysis section shall contain the calculations and/or empirical observations that will prove the design satisfactory (i.e. positive margins for all functional requirements for the circuit). The conditions which give true worst-case results shall be shown explicitly in this section. It is anticipated that only the most critical attributes of each circuit will be analyzed, but justifications must be given for all requirements not analyzed.

4.5.1 Parametric Variations Tabulation

The parametric variation for each part shall be a sum of the individual parametric variations due to end-of-life, radiation, part tolerance, temperature, and special piece part factors. Tables B-1 through B-9 contain recommended worst-case parameter variation for many component types and radiation test data is available from the references on a number of common devices.

When the analyst has knowledge that the physical configuration or operating mode constraints preclude the assumed simultaneous worst-cases, he (she) may gain relief by presenting the rationale for the use of his new values. For example, two digital gates in the same chip or two ICs on the same board cannot be simultaneously exposed to opposite temperature extremes.

4.5.2 Functional Blocks

The analysis should proceed through the circuit as a signal would flow from input to output. The contribution of each piece part to the worst-case output need not be discussed, but the calculations of cumulative contribution of each stage, sub-circuit, or functional block must be shown. The worst-case output from preceding blocks shall be used as the input to the next block. Circuits with feedback should be considered as a single block to reduce iteration time, where practicable.

4.5.3 Iterations and Summaries

Ideally, one pass through the circuit under worst-case conditions should give the worst-case output from the circuit. The analysis will determine the output of the stage/sub-circuit/functional block and define these to be the inputs to the corresponding next stage/sub-circuit/functional block. The outputs from the assembly/subsystem must then be compared with the requirements established per Section 3.0 and documented in Section 4.0 of this appendix.

4.5.4 Software Description

If the analysis has utilized any computer simulation or software, the description of the software should be included in this section and the method of parametric variation discussed unless the program is configuration controlled and available from either commercial, DOD or NASA sources.

4.6 Summary

This final section shall provide a summary of the analysis results and point out any deficiencies which the circuit worst-case analysis has revealed. The analysis section will contain all detailed analytical descriptions; the summary section will only serve to outline the results.

If the performance requirements have not been met in any instance, the deficiency must be stated. If the normal analysis assumptions have been perturbed (such as by RSS analysis, Monte Carlo, or modified environments) the reported results should note these caveats.

5.0 Circuit Specific Analysis Content

5.1 Digital Circuits Worst-case Analysis

5.1.1 Interfacing Digital Technologies

Whenever digital circuitry is not of a single technology type, all parts must operate properly together under simultaneous worst-case source and load conditions. It is suggested that particular attention be paid to noise margin at the interface. The defined input and output characteristics of various digital technologies are as shown in Table B-9. The specific devices of the various families, as noted in this table, are used in the timing examples of Section 5.1.2.

5.1.2 Timing

All sequential circuits should have a worst-case timing diagram made to determine the effects of variations in switching times of the installed devices. There are many factors which affect timing in digital circuits. These factors include supply voltage, capacitive loading, clock instability, and clock skew. An RSS or Monte Carlo analysis for timing margins is not allowed due to the catastrophic nature of failed timing.

5.1.2.1 Signal Delays and Response Times

The limits of the propagation delays for the circuit being analyzed must also be shown in the WCA. Response times for the circuit must comply with the required response times identified in the requirements matrix of section 4.4. For circuits which have no specified delay or response time requirements at the unit level, the worst-case response times should be explored at the system level to determine if design constraints should be levied "from the top down".

5.1.2.2. Digital ASIC

It is assumed that the end user (i.e., JPL design engineer) has defined the following in a digital ASIC specification:

a. Functional performance (i.e., logic functions);

b. Input/output signals, including their absolute and relative delays, levels, and rise times;

c. Input clock signals, including skews, duty cycles, and rise and fall times;

d. Supply voltage limits;

e. Noise immunity;

f. Environmental limits (i.e., temp, mechanical, radiation, life).

Verification that a fabricated design from a specific vendor meets the above requirements generally is an Office of Reliability Engineering responsibility since it is subject to the WCA process. The following nomenclature and definitions form an integral part of the WC verification process.

Hardware Design Language (HDL)

This is a subset of the programming language "C" which the JPL design engineer uses as a first step in converting the gate level hardware spec into a software definition of the functional building blocks. This is universal to all vendors and requires no action from 5X. "Verilog" is a commonly used HDL at JPL. Note that a manual approach using conventional schematic capture also may be used.

Technology File (TF)

This is sometimes described as the "Cell Library". It contains the simplest basic set of digital building blocks (primitives) from which all other more complex functions are constructed (e.g., AND, NAND, OR, NOR, FLIP FLOPS, etc.). As a part of the vendor selection process, Reliability Engineering should participate in a detailed review of the TF jointly with the engineers of the proposed vendor. Note that the vendor will have several TFs, depending on the following variables:

1. Manufacturing process (feature size, dopings, technology, etc.);
2. Operating voltage;
3. Operating temperature;
4. Radiation TID;
5. Minimum operating life (not always specified by vendor)

These TFs should specify guaranteed minimum and maximum delays for each cell (primitive). The Office of Reliability Engineering review should verify that adequate margin exists to accommodate the EVA sum of the above contributors to delay variation to assure that the min and max cell delays will be met (not including input or output wiring delays to or from the cells).

Intellectual Property (IP)

The IP is a software defined ("C" language) extension of the logic cells to perform a more complex digital function (e.g., shift register, counter, microcontroller, etc.), which uses large numbers of combined cells. The IPs may have been created by the JPL design engineer or purchased from a software design specialist as a licensed, copyrighted item. Note that there is no physical dimension and hence no delay definition inherent in the IP. It is simply an interconnection list (i.e., cell A output connects to cells B, C and D inputs). Because it defines only functionality of the logic and because that functionality is verified by other Built In Self-Test (BIST) exercises, 5X has no direct interaction with the IP.

The result of the design engineer having captured the complete functionality of the ASIC via a mixture of discrete cells and complex IP configurations, is either a "Gate Level Net List" (GLNL) or a data base in "Register Transfer Language" which defines the functional interconnections to and from each primitive. This is sent to the vendor together with test vector definitions and any other specific design constraints.

This package constitutes a part of the JPL procurement spec definition used by the vendor to design the digital ASIC. Note that all ASICs are defined also by a source control drawing generated by parts engineering. These include the max allowable screening deltas for environmental tests, radiation tests and life tests.

Net Delay Formulae (NDF)

The interconnection of cells requires real metallic conductors on multiple layers. As such, the dimensions and location of these conductors and layer to layer VIAs and insulators can effect electrical operation in the following ways:

a. Rise Time (width, length, height from ground, insulator dielectric constant);

b. Propagation Delay (conductor length, VIA length);

c. Erroneous Signal Coupling (cross-over geometries, parallel run geometries, rise times (dv/dt), cell maximum detection bandwidth (sliver susceptibility).

The Reliability Engineering analyst should review the vendor's NDF and its associated design/layout constraint rules to assure himself that the formulae used to calculate the above effects are correct and comprehensive enough to assure meeting the worst-case operating speeds while maintaining immunity from false triggering. Ground bounce performance should be studied for the max current, max capacitance, max length case.

Standard Delay Format (SDF)

After the HDL defined functionality has been converted by the vendor to a hardware layout of interconnected cells, a back annotated post layout database is constructed and is defined as the SDF. It contains the min and max delays of each cell and its associated conductor runs. Based on a very detailed study of the intended functionality of the ASIC, the Reliability Engineering analyst, with the concurrence of the design engineer, defines the "delay critical paths" for detailed examination. By using a static timing tool, such as "prime time", he can ask for the delay from point A to point B relative to a reference event C (clock edge, etc.). The timing tool will import the SDF file and extract and add the required delays to provide a WC min and WC max delay from A to B and WC set up and hold times. The analyst then compares these to the original JPL spec requirements at the ASIC input/output level and passes judgement on the design acceptability and its compatibility of timing with interfacing ASICS, memory devices, or data buses.

If not acceptable, the analyst should attempt to define the problem area by examining the physical layout and either recommend a relayout or other design change or defer the problem to the design engineer for more fundamental changes (spec or process).

Analysis Tasks and Associated Mandatory Access

Successful completion of a digital ASIC WCA requires the following tasks from the responsible analyst:

Task 1:	Review and acceptance of the applicable vendor cell library;
Task 2:	Review and acceptance of the vendor net delay formulae;
Task 3:	Identification of delay critical paths;
Task 4:	Verification of positive EVA timing margins for the critical paths, (temperature variations may be assumed as zero across the chip)
Task 5:	Report of results of Tasks 1 through 4.

Analysis Mandatory Deliverable Items

Assuming that Reliability Engineering (Office of Reliability Engineering) is required to perform a WCA of the ASIC (Task 1-5), the following items must be provided as input information via the procurement package.

a. The vendor “Standard Delay Format” file must be a contractually identified deliverable item in tape, CVD, or equivalent form.

b. The vendor contract must guarantee access to the “Technology File” and the vendor “Net Delay Formulae”.

c. The HDL file generated by the JPL design organization must be made accessible to Reliability Engineering for selection of critical paths and general understanding of the desired functionality in tape, CD, or equivalent form

d. The physical layout file must be supplied by the ASIC vendor to Reliability Engineering via design engineering

5.1.2.3. FPGA (Field Programmable Gate Arrays)

The analysis process steps are similar to those of the digital ASIC, but more of the responsibility for configuration lies with the user (design engineer). Good design practice requires the design engineer to create an FPGA specification with the same five items defined as for the digital ASIC. Spec conformance is usually a Reliability Engineering responsibility.

Vendor Design Language

Unlike the digital ASIC, the HDL is not a universal standard for definition of the FPGA. A vendor can create and supply his own design definition language. The trend is toward HDL.

Technology File

As in the digital ASIC case, the “cell library” must envelope the worst-case min and max performance required by the design engineer, including allocations adequate to cover radiation and life. Again, Reliability Engineering is responsible for interfacing with the vendor and assuring that the min and max propagation delays are conservatively defined.

Intellectual Property (IP)

These have the same definition as the digital ASIC, i.e. they are defined by the JPL design engineer. In this case, they are implemented also by the design engineer as he defines the interconnection map using the vendor-defined methodology. There is no direct 5X involvement in this process.

Net Delay Formula (NDF)

Reliability Engineering must review the vendor’s current net delay equations to assure that prop delays, rise times and coupling are correct and comprehensive.

Standard Delay Format (SDF)

Although the interconnections are JPL defined, the process of reviewing the “delay critical paths” is a Reliability Engineering responsibility and identical to the digital ASIC process.

Analysis Tasks and Mandatory Access

Identical to digital ASIC.

Analysis Mandatory Deliverable Items

a. The vendor contract should guarantee access to the vendor “Technology File” and the vendor “Net Delay Formulae”.

b. The interconnection file generated by the JPL design engineer must be made accessible to Reliability Engineering Office in tape, CD or equivalent format for selection of critical paths and general understanding of the desired functionality.

c. The “As-Burned” physical layout generated by design engineering must be made available to Reliability Engineering in tape, CD or equivalent form for use in delay computations

NOTE: The analysis functions identified as usually reliability engineering functions could be assumed by either the JPL cognizant design section or by parts engineering. In either case, the above noted “Analysis Mandatory” information items will still be required for a WCA and should be provided for as part of the procurement package.

5.1.3 Power Consumption

The power for individual components shall be tabulated in the part stress analysis. The WCA shall contain the total worst-case consumption of power. It is recommended that this power be expressed as both an EVA number and as an RSS value for individual subassemblies and at the assembly level. These values will be used in the judgment of power supply adequacy. Manufacturers data sheets or appropriate specification sheets usually contain device power consumption graphs. Power consumption can be affected by temperature, radiation total dose, and applied voltage; and all should be considered.

5.1.4 De-coupling

Each printed wiring board containing digital microcircuits should have been analyzed for lead inductances and appropriate decoupling capacitance added to compensate for the board inductance. Adequate capacitance must be provided to assure that the device will not be subject to peak power supply fluctuations. The adequacy shall be tested by showing that the sum of the DC variations, normal supply ripple, and local board induced fluctuations result in instantaneous voltages within the supplier's allowable operating voltages.

5.1.5 Miscellaneous

For devices which contain memory and are part of a state machine, (i.e. counters, registers, etc.) unused states must be defined and provision made for the release from this state without damage or fault generation. The effects of the device entering into one of these unused states must be evaluated and the clearing method outlined. For one-shot functions, the prevention of false triggering must be included in the WCA. Noise transients should not trigger the one-shot. When the one-shot functions as an interrupt driver, software should be checked for interrupt truth in its service routine to preclude the service of unprepared devices. The one-shot external timing components shall be selected such that the one-shot has a worst-case maximum and minimum pulse width which is within +25% of its nominal, and this tolerance shall be used as an input variation to its load circuit.

5.2 Switching Circuits Worst-case Analysis

5.2.1 Considerations

Switching circuits, such as those used in switching power supplies, servo drivers, and push-pull amplifiers are considered in this category. The critical function is the positive switching of the desired signal and the lockout of the complementary switch during crossover. Parameters requiring attention are the rise and fall times of the switches, transient conditions, switch stress during peak power delivery, and output impedance matching (for efficiency). The WCA shall also consider the power-up and power-down states of the switching circuit to assure that no loss of accuracy or overstress occurs during these intervals.

5.2.2 Solid State Switching

The use of transistor switches to implement signal transfer is common and requires special analyses. In general, solid state switching circuits function as power switches, either in continuous or pulsed mode. The smooth delivery of this power with low distortion is critical to the circuit's proper operation. The following items should be checked by the WCA.

5.2.2.1 Switching Transistors.

The operation of transistor switches shall be within the safe operating limits for all worst-case loads. The locus of I-V operating points shall fall into the derated, safe operating regions from the device specification. The average dissipated power in the switching transistors shall be determined from the sum of the operating, quiescent, and transitional power dissipations. Switches not used in the push-pull mode are to be analyzed for their dissipation of power with worst-case loads and drive circuitry characteristics.

5.2.2.2 Drive Circuitry.

Drive circuits are to be examined for crossover overlap in push-pull configurations. If the possibility of both switches being on at once is found, steps must be taken to control the current through the output stage and bring the overlap under acceptable control. The power dissipated in the case of crossover shall be calculated as input to the stress analysis.

5.2.3 Electromechanical Switching

A WCA or appropriate test data should demonstrate that relay or solenoid drive circuitry precludes the possibility of "hang-up" in a state between set and reset. The WCA should consider the worst-case EM device, drive circuit and environmental conditions. The analysis should also verify that coil power is not routed through its own contacts.

It should be verified that the assumed source of power is well regulated and does not suffer voltage droop as a result of the relay event (such as a capacitor bank or an inductive source). Any RC timing circuits used to control applied coil energy should be analyzed. The presence of adequate coil and contact suppression should be verified. A common WCA report section should summarize the analysis results of all included relays.

5.2.3.1 Drive Circuitry

Drive circuitry for the electromechanical switching circuits is not often subject to crossover. In most cases, relays are used to make one-time, contact to transfer power or control to some assembly or device. The drive circuitry must satisfy all expected worst-case conditions such as pickup and dropout voltage and reaction times, over the limits of coil resistance, temperature and any applied mechanical loads. The drive circuits must also supply pulses of sufficient width to insure latching.

5.2.3.2 Contact and Load Considerations

Load considerations for electromechanical switching must be delineated in terms of the type of load, the amperage to be delivered, suppression (if any) of RFI, contact voltage drop, and load tolerance to contact bounce. The switching of the device shall not degrade the load operation due to transients or bounce generated by the switch. It is the responsibility of the switch designer to inform the down stream user of the expected transients.

Contact capability is usually specified to guarantee that the contact resistance stays below X ohms at a defined current after a defined number of operations. For purposes of WCA, the designer should assure that the number of intended mission operations is less than the device specified value. Even if the actual operations are far less than the specified, the maximum defined contact resistance should be used in the WCA while adhering to the current derating requirements.

5.3 Analog Circuits Worst-case Analysis

5.3.1 Considerations

Analog circuits include functions such as amplifiers, signal generators, line drivers and receivers, integrators, and other signal conditioners. Parameters which are important to these circuits are described below.

5.3.2 Amplifiers

Amplifiers must operate properly under worst-case conditions of power supply voltage, load, and peripheral component degradation. Amplifiers shall meet their requirements for gain, stability, distortion, phase-gain margin, linearity, common mode rejection ratio, noise rejection, and offset voltage.

5.3.3 Signal Conditioning

If the circuit does any conditioning of the input signal such as amplitude limiting differentiation, integration, or active filtering, the performance of that conditioning must be assured for worst-case conditions. For these types of signal conditioners, the controlled distortion (shaping) of the input signal is the primary function of the circuit. The worst-case loading of these signal conditioners can affect that function and must be considered.

5.3.4 Hybrid Circuit Assemblies

A hybrid circuit is defined as a functional group of parts housed in a hermetically sealed assembly using a common ceramic substrate as it’s mounting and interconnection medium. The complexity may vary from a single amplifier made from discrete parts on a single layer of ceramic to a multi-chip module (MCM) using several interactive ASICs on a multi layer ceramic structure with hundreds of connections.

WCA Responsibilities for Origination and Review

The following table describes the possible choices in responsibility for origination and review of the WCA for hybrids:

Design	Fabrication	Originate WCA	Review WCA
JPL, DE	JPL	JPL, DE +RE	NA
JPL, DE	Vendor	JPL, DE +RE	NA
Vendor, DE	Vendor	Vendor	JPL, RE

DE = Design Engineering Organization

RE = Reliability Engineering

Assumptions:

1. Any ASICs or FPGAs have been WCA analyzed previously using the methods described in those WCA sections.

2. A very detailed thermal analysis or IR measurement has been completed as a part of the stress analysis activity and all derating requirements have been met. The thermal analysis resolution should be no larger than the smallest part.

3. A comprehensive spec exists describing the required performance at the input/output pins of the hybrid.

4. Part specs exist for all electronic parts used in the hybrid.

Methodology

a. The analyst must derive a part level WC part parameter database unless already specified by a WCA project specific database exists. It must include all effects (temp, Rad, aging, voltage, etc). Concurrence of the part data base values by Parts Engineering is required.

b. If applicable, all critical timing interactions must be verified to have positive margins using an EVA analysis.

c. All critical frequencies, bandwidths and signal levels must be verified. For high speed logic and RF signal circuits (>10 MHz) the geometries of ground planes, intrahybrid connection wires and terminals as well as circuit input and output impedances must be used to calculate transmission line effects. The results should verify adequate signal fidelity and the avoidance of detrimental voltage bounce on grounds and supply lines.

Note that for analog circuits, a three sigma statistical result is considered adequate performance unless specified otherwise by the project. For digital circuits, critical timing must produce positive margins in an EVA analysis due to the potentially catastrophic effects of a failure.

Documentation

A comprehensive WCA document must be produced for each hybrid assembly.

5.4 RF Circuits Worst-case Analysis

5.4.1 Considerations

RF circuits shall be analyzed for worst-case response under AC, DC, and transient modes of operation. The analysis shall take into account all worst-case variations in components due to temperature, voltage and frequency tolerance, aging, manufacturing tolerance, and radiation degradation.

RF circuitry functions in many differing configurations. As such, the guidelines for RF circuitry will be listed rather than explained. The lists give some of the parameters thatthe WCA could address, although not necessarily the only ones.

5.4.2 RF Amplifier Parameters

Bias and/or operating point

Dynamic range (input and output)

Input/output impedance (magnitude and phase)

Input/output VSWR

Gain/phase stability

Feedback stability margins

Frequency response (bandwidth, flatness)

Compression points

Power Dissipation

5.4.3 Oscillator Parameters

Frequency stability and accuracy

Output power level and stability

Spectral purity

Phase stability and locking accuracy

Signal isolation

Output impedance/load impedance match

Noise and stray RF control

5.4.4 Comparator Parameters

Threshold precision

Switching, speed/time constant

Hysteresis

Offset stability

5.4.5 RF Switches

Power dissipation

Switching speed

Power capacity

Drive requirements

VSWR

Insertion loss

Frequency response

Video feed through

Isolation

Input/output impedance and matching

5.4.6 Mixers

Noise figure

Frequency response

Drive levels

Compression points

Intercept points

Group delay

Isolation

Power dissipation

Spectral purity

Conversion loss

Port impedances

Intermodulation distortion

5.4.7 Filters

Insertion loss

Frequency response and bandwidth

Input and output impedances and matching

VSWR (input and output)

Phase linearity

5.4.8 Coupler and Circulator Parameters

Insertion loss

Frequency response

Power capability

Isolation

Directivity

Magnetic leakage

VSWR

Input and output impedances

5.4.9 Stripline, Waveguide, and Cavity Parameters

Mode suppression

Insertion loss

Dimensional stability, aging, environmental effects

Input and output impedances

VSWR

5.4.10 Modulator Parameters

Frequency response

Input and output impedances

Insertion loss

Output spectrum

Phase response and linearity

Output level

VSWR

5.4.11 General Parameters

Power supply decoupling

EMC

5.4.12 Multiplier Parameters

Input and output impedances

Input drive levels

Output power

Isolation

Frequency response

Output spectrum

5.4.13 Detector Parameters

Bias voltage

Frequency range

Input and output impedance

Input VSWR

5.4.14 Power Splitter Parameters

Insertion loss
VSWR
Input and output impedance
Power handling capability
Frequency response
Imbalance

5.5 Power Conditioning Circuits Worse Case Analysis

5.5.1 Considerations

Typical electronic circuitry usually requires the conditioning of power from a noisy, poorly regulated source to a load which demands highly regulated well-filtered voltage or current. The following sections provide a discussion of possible topics for analysis although it is anticipated that the typical WCA will address only the most critical of these as dictated by the specific application. Because of the complexities and non-linearities inherent in power conditioning, inputs to the part stress analyses are complex and therefore usually performed by the WCA analyst. Computations of the internal workings of magnetic elements are necessary only if they are not procured to a source control specification.

5.5.2 Regulation

Determine the worst-case regulation limits under line, load, environmental and life extremes. For switching regulators, consider the effects of ripple on regulation. If output filters are used, the output voltage variation due to load changes should be evaluated.

5.5.3 Efficiency

The power dissipated within the supply should be determined, and the efficiency calculated at minimum load, maximum peak load and maximum steady state load to show compliance with the input power and efficiency requirements.

5.5.4 Transient Response

Power supply transient response should be determined due to line changes, load changes and power on/off operations. The following effects shall be investigated.

(1) Outputs. Determine the maximum/minimum output voltages and response times. In particular, the possibility of output overshoot should be considered.

(2) Stress. Additional stress imposed by transients should be determined. In particular, the start current, voltage, and power transients should be shown to be less than the safe operating limits of the switching transistors.

(3) Magnetic Saturation. Transient conditions should be analyzed for the possibility of unwanted magnetic element saturation.

(4) Inrush. The maximum inrush current and energy at power up should be determined and compared with requirements.

5.5.5 Operating Frequency

The designer shall determine the worst-case operating frequency and duty cycle limits for line, load, temperature, end of life extremes, and radiation effects. Internal oscillators shall be analyzed for frequency stability. Freedom from possible mode shift to sub or multiple harmonics should be demonstrated.

5.5.6 Starting

It shall be verified that the switching power supply can start under all worst-case conditions. Normally temperature extremes, maximum DC load, and maximum capacitance represent worst-case conditions.

5.5.7 Switching

Switching transistors shall be analyzed in detail in order to demonstrate that switching is performed in a predictable and consistent manner under all worst-case conditions, and that the drive to the switching elements is adequate. The drive circuit analysis should show that both switches in a two switch drive stage cannot be on simultaneously, or that current limiting is provided during intentional simultaneous conduction. The impact of transistor crossover and of crossover protection circuits on switching and on regulation should be investigated and the additional power dissipation due to crossover calculated.

5.5.8 Inductor and Transformer Considerations

Magnetic drive stages shall be shown to have adequate suppression under worst-case voltage and duty cycle conditions.

Transformer applications shall be analyzed for the possibility of DC imbalance. The primary open circuit voltage and the secondary imbalance current shall be determined, and the resulting stress on the switching transistor due to the imbalance shall be assessed.

The possibility of zero current inductor (dry choke) operation in switching regulators should be investigated. If a zero current condition can exist, the effect on output ripple voltage, capacitor ripple current, output regulation, frequency and stress must be investigated. Control loop stability must also be investigated for modes of operation which include zero current in the output inductor.

The possibility of the output transformer magnetizing current being greater than the load current should be investigated.

5.5.9 Filtering and Stability Considerations

In general, special precautions must be taken to prevent peak detecting of outputs under light load. Peak detecting is caused from output transformers having excessive leakage and inductance in the secondary/primary windings or discontinuous inductor current.

Power supply phase and gain margin shall be determined by an open loop frequency response analysis. The allowable worst-case phase margin shall be assumed as 30 degrees and the allowable worst-case gain margin assumed as 10 dB, unless specified otherwise. The possibility of power supply instability caused by an input filter loaded by the negative impedance presented by a switching regulator input should be investigated.

The possibility of polarized filter capacitors becoming reverse biased at power down shall be prevented. If reverse bias occurs, the consequences shall be determined by considering the type of capacitor, the magnitude of the reverse bias voltage and the level of the breakdown current flow.

Capacitor ripple currents shall be determined. Ripple currents in the input and output filter capacitors are especially critical. The ripple current shall not exceed the derating requirements.

The effect of voltage transients during switching intervals should be determined. Suppression of inductors subject to being open circuited should be analyzed to verify the limiting of transient voltages to acceptable levels, as dictated by part stress derating criteria.

5.5.10 Second Breakdown

All power transistors, switching or linear, should be analyzed for forward-bias and reverse-bias second breakdown and compared to the safe operating area requirements for the maximum junction temperature.

5.5.11 Protection Circuits and Their Trimming

The worst-case overvoltage, undervoltage, and overcurrent set point ranges should be verified relative to the power supply and load circuit requirements. The overcurrent results should be reported as a part of the power system analysis.

The trimming procedure should be analyzed in detail. Output voltage, overcurrent set point, overvoltage set point and undervoltage set point trim procedures should be considered. Input voltage, environments, loads on all outputs and the trim tolerances (e.g., EOL and setting resolution) should be included. The resistor range and increments shall be verified to provide the desired trim tolerance.

5.5.12 Magnetics WCA

For magnetic devices not purchased to a source control spec, the analyst should determine the minimum and maximum inductance as a function of temperature, initial tolerance, DC magnetic field intensity (oersteds) and peak flux density (gauss). In some instances, as in tape wound cores, the inductance has little meaning. In such cases, magnetizing current should be measured under anticipated operating conditions.

Show that the worst-case transformer core maximum flux density (Bm) is not exceeded. Temperature, minimum frequency and maximum voltage must be considered. An example of a transformer requiring this analysis is a DC/DC converter output transformer. Special attention must be given to the temperature dependence of Bm when using ferrite cores.

Determine the circular mil per ampere actuals (CM/AMP) for all inductor and transformer windings. The maximum allowable current density in copper is 500 CM/AMP. In some instances, this can be exceeded provided that a thermal analysis is performed on the magnetic device.

Winding resistance should be measured or calculated. The resistance should be adjusted for temperature by the copper resistivity temperature coefficient.

6.0 Part Parameter Variations

The preferred approach to part variations is the development of a project unique part parameter variation handbook. This process provides a uniform data source for all design engineers and analysts which encompasses the specific life, temperature, and radiation environments of the project and its approved part list. The methodology is given in detail in JPL D-10133. If project constraints preclude a detailed data-base; the following tables will provide a recommended variations to be used for a program with an anticipated unpowered life of three years at room ambients from the time of part purchase to flight, and an assumed powered life of three years for test and flight at an assumed 95°C part temperature and with semiconductor junctions of 110°C. (Note: For programs where the times and temperatures vary from these values, parameter variations may require adjustment). Life effects may be scaled as the square root of the mission duration in the absence of any life test data.

The total variations listed are for part ambients from -35°C to + 95 °C when combined with life, mechanical stress and electrical stress effects. They do not include radiation effects which will be additive. Single event upsets (SEU) analysis will be treated in a separate analysis. Any deviations from the tabulated variations should be substantiated by modified environment or specific device test data or modified analytical techniques (RSS, Monte Carlo, etc.). For parts not listed here, the analyst may either derive his own values or confer with JPL Reliability for assistance.

Table B-1. Worst-Case Parameter Variations for Transistors

Parameter	Variations	Conditions	Remarks
hFE (Note 1)	+0.9%/°C *	For temperature	Change from design value mfr. spec.
	-10%	For life	Not additive to rad. effects.
VCE(SAT) (Note 2)	+15%	For life	Change from max. value in mfr. spec.
	+0.2mV/°C	For temperature	
VBE(SAT)	+15%	For life and temperature	Change from max. value in mfr. spec.
ICBO	doubles every 10°C increase	For temperature	Change from max. value in mfr. spec. at 25°C.
	+50%	For life	Not additive to rad
IEBO	doubles every 10°C	For temperature	Change from max. value in mfr. spec. at 25°C.
	+50%	For life	Added to temperature effects - not additive to rad effects.
ICES	3OX	For life and temperature	Change from max. value in mfr. spec.
tr (1)	+10%	For life and temperature	Change from max. value in mfr. spec.
td (1)	+10%	For life and temperature	Change from max. value in mfr. spec.
ts (1)	+10%	For life and temperature	Change from max. value in mfr. spec.
tf (1)	+10%	For life and temperature	Change from max. value in mfr. spec.
Cobo (1)	+5%	For life and temperature	Change from max. value in mfr. spec.
Cibo (1)	+5%	For life and temperature	Change from max. value in mfr. spec.
fT (1)	-5%	For life and temperature	Change from min. value in mfr. spec.

* Manufacturer's data may be used when available.

NOTE 1: hFE max @ 25°C = 2.5 x HFE nom @ 25°C unless specfied otherwise by the vendor.

NOTE 2: VCE(SAT),min shall be assumed equal to zero.

NOTE 3: Minimum values shall be assumed equal to 50% of nominal or 33% of maximum if not specified.

Table B-2. Worst-Case Parameter Variations for Resistors

Part description: General, class, type	Manufacturer's type number	Tolerance, % Initial	Design (a ,b)
Carbon comp.	RCRO5,7,20	+5	+20
Precision WW	HR series	+0.1	+0.4
	RBR series		
Metal film	RNC55H	+1	+2
Metal film	RNC50H	+1	+2

a) Design tolerance includes purchase, temperature, and end-of-life tolerances except where noted.

b) Design tolerance does not include voltage coefficient effects for which mfg. spec. should be consulted.

Table B-3. Worst-Case Parameter Variations for Fixed Capacitors

Part description: General, class, type	Part type number	Tolerance (in +/- %)	
		Initial	Design (a)
Solid tantalum	CSR13-KS	5	15
Solid tantalum	CSR13-KS	10	20
Ceramic	CKR05BX-KS	10	33
Ceramic	CKR05BX-KJ	10	25
Ceramic	CKR11BX-KR	10	25
Ceramic	CKR12BX-KR	10	25
Ceramic	CKR14BR-KR	10	30
Ceramic	CKR15BR-KR	10	30
Ceramic	ML10 MC70	5	6
temp. comp.	ML11 MC90		
Ceramic, HV disc.	800 series	10	17
Glass	CYFR series	1	2.1
Porcelain	VY series	10	11

a) Design tolerance includes purchase, temperature, and end-of-life tolerances except where noted.

Table B-4. Worst-Case Parameter Variations for Diodes

Parameter	Variations	Conditions	Remarks
VF	+1%	For life	Change from initial value.
	+150 mv	For temperature	
c	+25%	For life and temperature	Change from value in mfr. spec.
tr	+10%	For life and temperature	Change from value in mfr. spec.
IR	5X	For life	Change from value in mfr. spec.
	2X For every l0°C	For temperature	Change from value in mfr. spec.

Table B-5. Worst-Case Parameter Variations for Zener Diodes

Parameter	Variations	Conditions	Remarks
VZT	±2%	For life	Added to tolerance in mfr. spec.
ZZT	+10%	For life and temperature	Change from value in mfr. spec.
TC	+10%	For life and temperature	Change from value in mfr. spec.
IR (Below knee)	30X	For temperature	Change from value in mfr. spec.
	10x	For life	
VF	+10%	For life and temperature	Change from value in mfr. spec.

Table B-6. Worst-Case Parameter Variations for Zener Reference Diodes

Voltage referenced diodes

Parameter	Variations	Conditions	Remarks
VZT	±0.25%	For life	Change to tol. in mfr. spec.
IR (Below knee)	30X	For temperature	Change from value in mfr. spec.
	10X	For life and temperature	
ZZT	+10%	For life	Change from value in mfr. spec.
Temp. Coef.	+10%	For life	Added to mfr. Temp. Coefficient

Note: Consult with part specialist on life stability factors.

Table B-7. Worst-case Parameter Variations for Bipolar Integrated Circuits

DIGITAL IC's (TTL AND LOW POWER TTL)

Parameter	Variations	Conditions	Remarks
IIN(H)	+75%	Life and temperature	
IIN(L)	+20		
IOUT(H)	-20		(Source capability decreases for same VOUT spec)
IOUT(O)	-20		(Sink capability decrease for same VOUT spec)
IOS	+25		
TPDH	Table B9		
TPDL	Table B9		
Icc	+25		
Clock pulse width (input)	+25		

LINEAR IC'S

Parameter	Variations	Conditions	Remarks
AV	-40%	Life and temperature	
VOS	+20%		
IIN	+30%		
EO	-10%		
IBIAS	+10%		
VOS/T	+40%		
IOS	+10%		
Icc	+10%		
IEE	+10%		

Table B-8. Worst-case Parameter Variations for CMOS Integrated Circuits

Parameter	Variations,% (life)	Variations (temperature)	Remarks
IOUT(H), (L)	-10	-20%	Source capability decreases for same VOUT spec.
ISS	+50	+10	Quiescent Current
TPLH	+5		Change from max
TPHL	+5		Value in mfr. spec

Table B-9 Electrical Characteristics

Electrical Characteristics

<table>
<tr><th></th><th>Source</th><th>V_{CC}</th><th>V_{OH}</th><th>V_{IH}</th><th>V_{OL}</th><th>V_{IL}</th><th>I_{OH}</th><th>I_{IH}</th><th>I_{OL}</th><th>I_{IL}</th></tr>
<tr><td>TTL (SN5400)
R_L –Dominated</td><td>1</td><td>@5V</td><td>2.4V</td><td>2.0V</td><td>0.4V</td><td>0.8V</td><td>-0.4mA</td><td>40uA</td><td>16mA</td><td>-1.6mA</td></tr>
<tr><td>LSTTL (SN54LS20)
R_L –Dominated</td><td>1</td><td>@5V</td><td>2.4V</td><td>2.0V</td><td>0.4V</td><td>0.7V</td><td>-0.4m</td><td>20uA</td><td>4mA</td><td>-0.4mA</td></tr>
<tr><td>HCMOS (SN54HC00)
C_L -Dominated</td><td>3</td><td>@4.5V</td><td>4.4V
3.7V</td><td>3.15V</td><td>0.1V
0.4V</td><td>0.9V</td><td>20uA
-4mA</td><td>1000nA</td><td>20uA
4mA</td><td>-1000nA</td></tr>
<tr><td>4KCMOS (CD40118)
C_L -Dominated</td><td>2</td><td>@5V</td><td>4.95V</td><td>3.5V</td><td>0.05V</td><td>1.5V</td><td>-1.0mA</td><td>1000nA</td><td>0.9mA</td><td>-1000nA</td></tr>
<tr><td>HCT (SN54HCT189)
C_L -Dominated</td><td>3
5</td><td>@4.5V</td><td>4.4V
3.7V</td><td>2.05V</td><td>0.1V
0.4V</td><td>0.8V</td><td>20uA
-4mA</td><td>1000nA</td><td>20uA
4mA</td><td>-1000nA</td></tr>
<tr><td>AS (SN54AS00)
R_L –Dominated</td><td>4</td><td>@5V</td><td>3.0V</td><td>2.0V</td><td>0.5V</td><td>0.8V</td><td>-2mA</td><td>20uA</td><td>20mA</td><td>-0.5mA</td></tr>
<tr><td>ALS (SN54ALS00A)
R_L –Dominated</td><td>4</td><td>@5V</td><td>3.0V</td><td>2.0V</td><td>0.4V</td><td>0.7V</td><td>-0.4m</td><td>20uA</td><td>4mA</td><td>-0.1mA</td></tr>
<tr><td>HCS (Later)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="5"></td><td colspan="6">ALL DATA @ 25#C</td></tr>
<tr><td colspan="5">Compatibility Requirement</td><td colspan="3">Sources:</td><td colspan="3">1. TI TTL Data Book, Vol. 2</td></tr>
<tr><td colspan="5">$V_{OH} > V_{IH}$</td><td colspan="3"></td><td colspan="3">2. RCA CMOS Data Book</td></tr>
<tr><td colspan="5">$V_{OL} < V_{IL}$</td><td colspan="3"></td><td colspan="3">3. TI HCMOS Data Book</td></tr>
<tr><td colspan="5">$I_{OH} > I_{IH}$ (Sum of all loads)</td><td colspan="3"></td><td colspan="3">4. TI ALS/AS Data Book</td></tr>
<tr><td colspan="5">$I_{OL} > I_{IL}$ (Sum of all loads)</td><td colspan="3"></td><td colspan="3">5. RCA QCMOS Data Book</td></tr>
<tr><td colspan="5"></td><td colspan="3"></td><td colspan="3"></td></tr>
</table>

Appendix C - Electronic/Electromechanical/Electrical Parts Stress Analysis Guidelines

This Appendix is a guideline that identifies parts applications limitations and the data to be developed in performing a parts stress analysis. The application analysis shall be performed to verify that the applied stresses on the components at qualification test temperature levels do not exceed the applicable parts stress derating guidelines. In the analysis, it shall be assumed that the unit/assembly baseplate is set at the high qualification or protoflight temperature limit. The piece part operating temperature should then be determined by thermal analysis.

The stress analysis report shall contain all schematics and other applicable drawings with number and revision letter, as applicable to the analysis. Documentation requirements are discussed in Section 2.2. The derating limits per part type are defined in JPL D-8545, refer to the latest revision in the DMIE.

The detailed JPL stress sheets or their equivalent should be provided in any stress analysis submission. An electronic version of the forms containing the similar information can be developed by an analyst to simplify the implementation process.

APPLICATION DATA: Capacitors & Filters

The AC rating of a capacitor is influenced by capacitance, dissipation factor, mass, geometric configurations, and the ambient operating temperature. The following basic rules should be considered for ac applications:

(a) The capacitor should be packaged to maximize the heat dissipation capability of the device.

(b) Current limiting should be applied to the extent that it does not deteriorate the required circuit performance.

(c) Do not apply peak ac voltages that exceed the recommended dc rating of the capacitor.

(d) Determine if the capacitor is corona-free when the applied voltage exceeds

Exceptional Application Requirements For charge/discharge, energy storage applications, the following additional information is required:

(a) Pulse width

(b) Repetition rate

(c) Rise time

(d) Maximum charge/discharge current

APPLICATION DATA: Diodes and Transistors

Exceptional Application Requirements The following temperature-compensated zener reference diodes have minimum temperature rating of 0 °C rather than -55°C.

IN935 through IN946
FCT 1021, 22, 25
IN2620 through IN2624

APPLICATION DATA: fuses

The DC derating factors for fuses must be varied per fuse size according to the following table.

Fuse Current Rating (amperes) @ 25°C	Fuse 1/ Current Rating (amperes) @ 95°C	Derating 2/ Factor for Vacuum and Reliability on PC Board	Max AllowableDC Operating Current in Vacuum @ 95°C
15	13.2	0.5	6.6
10	8.8	0.5	4.4
5	4. 4	0. 5	2. 2
2	1.76	0.5	0.88
1	0.88	0.45	0.40
1/2	0.44	0.4	0.18
3/8	0.33	0.35	0.12
1/4	0.22	0.30	0.066
1/8	0.11	0.25	0.027

1/ Based on 0.2%/C° for medium and fast blow fuses.

2/ Derating factors are based on data from fuses mounted on printed circuit boards in vacuum and conformally coated. For other type mountings or pulsed waveforms, consult the project parts engineer for recommendations.

APPLICATION DATA: Inductors and Transformers

(1) Current density shall be less than 1 ampere per 500 circular mils, unless proved safe by a detailed thermal analysis.

(2) Temperature hot spots shall be determined based on the manufacturer's computed, measured or guaranteed max temperature rise from the part mounting surface to its hot spot. Typical good designs will limit the rise to 20 °C.

APPLICATION DATA: Integrated circuits, digital

(1) Input Current

(a) TTL input current at terminated, unused inputs shall be 100 microamperes or less.

(b) CMOS input current shall be externally limited to 10 milliamperes or less if driven when VDD-VSS is zero. The parts can be damaged if this is not done.

(c) Unused inputs of CMOS devices should be pulled to either V DD or VSS, whichever is appropriate for the logic circuit involved, and may be directly connected without current limiting provided that its own supply is used for the pull-up.

APPLICATION DATA: Relays

(1) Predominant dc switching functions.

(a) Coil. Characteristics of coil drive current and/or voltage shall be noted; e.g., in a pulse operated mode the current wave form should be supplied or in an unregulated drive voltage mode the voltage range should be defined. General limits are manufacturer's rated normal values.

(b) Contacts. For reliability, the contacts should be using the factors which account for temperature, load application and cycle rate.

Special Requirements

The relay electronic drive circuitry must be designed so that under no circumstances the following conditions could arise:

(a) Relay hangs up in midpoint and opens the coil drive circuitry.

(b) Relay cannot be reset.

In general, this requirement will restrict the use of interconnecting relay contacts for coil drive purposes and also restrict the use of timing circuits when proper circuit operation requires relay reaction times for proper switching.

APPLICATION DATA: Resistors

Exceptional Application Requirements.

(1) Power stress. Resistors generate heat, and one critical area of analysis is to determine how that heat is dissipated. Anything which lowers the element temperature of the resistor, decreases the stress on the part. For example, an Allen Bradley resistor operating at 150% rated power at 0°C ambient is stressed less than the same part operating at 50% power and 70°C ambient. Generally, 50% derating is recommended. Carbon composition and film resistors can safely be operated at 70% if the ambient temperature is 50 °C or less. Power resistors should never be operated at greater than 50% average power, and the chassis mount parts may have to be even further derated, depending on the available heat sink.

(2) Pulse power. Individual cases have to be evaluated. Conservatively, for all non film resistors, no problems can be expected at 100 times rated power if the single pulse power, when averaged over the thermal time constant period, is less than the rated DC power. A safe minimum value for thermal time constant is 1 sec. Some resistors have thermal time constants up to 1 min for the larger devices. Film resistor peak power should not exceed 4 times rated power unless specifically allowed in writing by the manufacturer.

Appendix D - Fault Tree Analyses Guidelines

1.0 Introduction

A comprehensive program to anticipate nearly all identifiable causes of failure and endeavor to prevent their occurrence can be used to insure that hardware will achieve a high level of reliability. The program is initiated by developing a comprehensive fault tree where the user strives to identify all of the possible failure causes of a specific failure These failure causes are compiled and combined with the prevention measures of the program to form a matrix. The fault tree and the prevention matrix-form are the two essential tools of this program. The fault tree is used for the identification of critical fault paths. The matrix-form is used to identify additional analysis, testing, or inspections needed for failure prevention.

To provide the level of detail required, the failure causes that can occur from the interworking of the mechanical piece parts, as well as those failure causes from the operating environment acting on the individual piece parts, must be identified. The program is flexible and can be applied successfully to many types of equipment, including the following: mechanical, electromechanical, photodetector, blanket, and heater. When properly applied, the fault tree/matrix-form program will appreciably reduce the probability of failure during equipment use.

2.0 Fault Tree/Matrix-Form Preparation

There are three steps in the fault tree and matrix-form preparation program:

1. The evolutionary compilation of discrete modes of failure and their associated causes, using a detailed fault tree.

2. The development of the corresponding matrix-form that combines the "generated failure causes from the fault tree" with the "planned preventive measures of the program."

3. Concurrence by the design agency that the applicable preventive measures regarding the matrix items either are, or will be, part of its reliability program. This concurrence must be among individuals in analysis, design, quality assurance, manufacturing, and/or other disciplines involved in delivering the equipment.

A brief description of each of the program's three main steps is given below:

2.1 Step 1: The Fault Tree

A fault tree analysis (FTA) can be described as an analytical technique, whereby an undesired or failed state of the system is specified, and all credible ways (faults) that the operating environment and/or lower levels of the system can cause this state to occur are identified. The fault tree (FT) itself is a graphical model of the system, which shows the logical interrelationship of the faults in the lower levels of the system. A fault tree thus depicts the logical interrelationship of basic events that lead to the undesired event, which is the top event of the fault tree. These faults can be associated with component hardware failure, human errors, or any other pertinent events which can lead to the undesired or failed state. It is important to realize that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to a specific top event, thus includes only those lower level faults that contribute to that top event. Thus, if there is more than one undesired or failed state of the system, a fault tree for each should be developed.

Fault tree methods should be applied in the early design phase, and then progressively refined and updated as the design evolves to track the probability of an undesired event. Initial fault tree diagrams might represent functional blocks (for example, units, or equipments), becoming more definitive at lower levels as the design materializes in the form of specific parts and materials.

Potential applications for the results of a fault tree analysis are shown in Table D-1. The input data requirements for performing an FTA are summarized in Table D-2. Figure D-1 shows an example FT with some possible types of faults that would lead to the postulated failure.

The first step in formulating the FT is the choice of an observed subsystem level functional fault (e.g., antenna fails to move, scan mirror failure, etc.). This functional fault is then the top level of the Fault tree. The analyst must then postulate the various lower level faults or failures which, individually or in combination, lead to the next level fault in question. As a rule, the FT should be expanded down to the level at which preventive measures can be affected. This level will most often be to that of the failed mechanical component (i.e., motor, bearing, shaft, etc.) excepting parts which are internal to procured items and which are not specifically called out in detailed specifications of the item.

The use of logical "AND" and "OR" symbols graphically depicts the combination of mechanical faults which lead to the observed higher level fault. The "AND" symbol means that the failures which feed into it on the FTA must both occur for the observed higher level fault to occur. The "OR" symbol means that either of the failures which feed into the symbol will cause the observed higher level fault to occur.

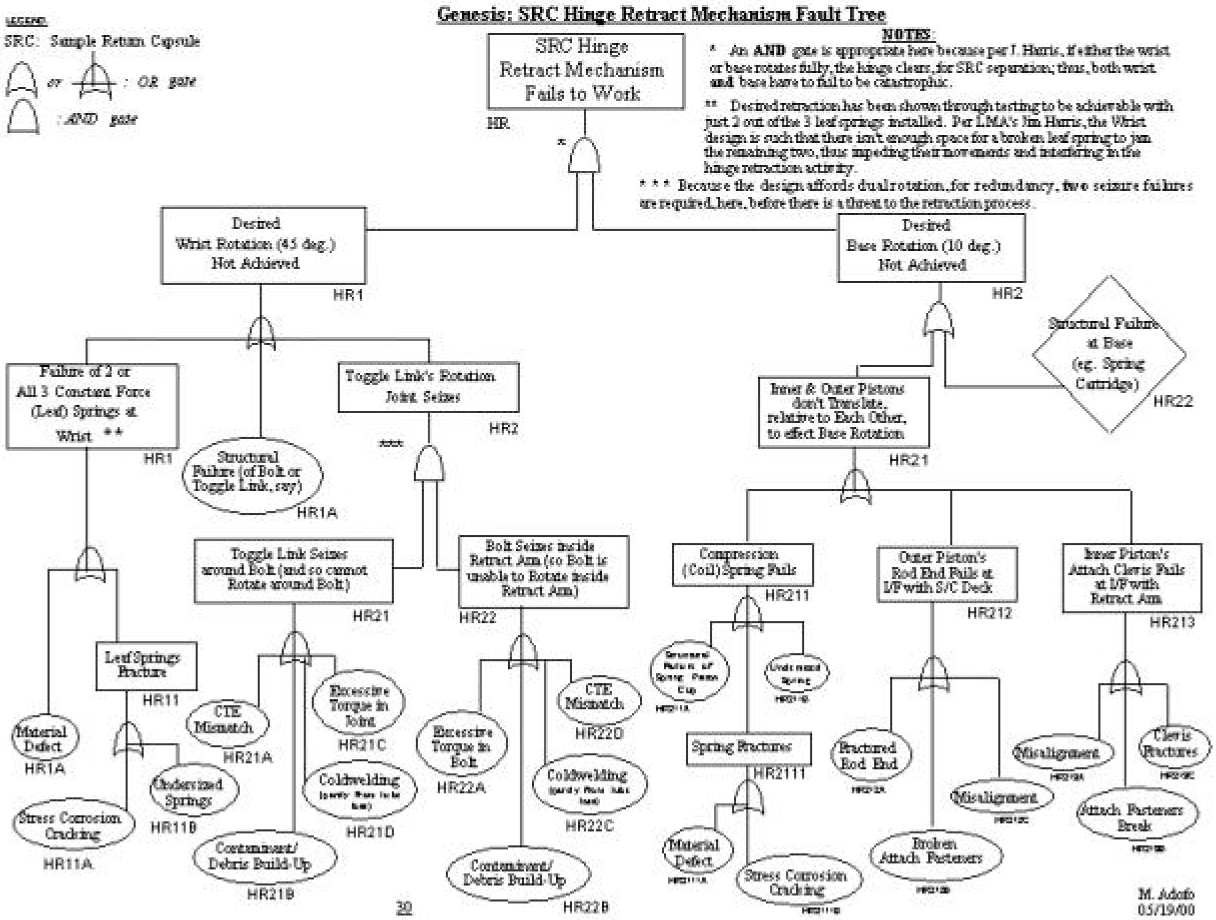
Events or observations related to the fault are, as the fault itself, put into rectangular boxes. An event or observation which is described by a basic system, component or part failure is put into a circle. Events or observations that are terminations of the fault sequence (for reasons of lack of sufficient information or to indicate further development) are put into diamond shaped parallelograms. These circles, boxes, and diamonds are logically connected by the logical "AND" and "OR" gates in pursuit of the description of the relation between the lower level and upper level faults.

Table D-1. Applications for FTA Results

1.	Early and continuous risk assessment for overall project risk management activities supported by mission level FTA
2.	Allocation of critical failure mode probabilities among lower levels of the system
3.	Comparison of alternative design configuration from a functionality or safety point of view
4.	Identification of critical fault paths and design weaknesses for subsequent corrective action
5.	Evaluation of alternative corrective action approaches
6.	Development of test, maintenance, and operational procedures to recognize and accommodate unavoidable critical failure modes

Table D-2. Input Requirements for an FTA

1.	Definition of events and interconnections
2.	Definition of the principle postulated fault and its modes of failure
3.	Definition of applicable possible human errors
4.	Equipment design information
5.	Definition of the maintenance concept for the equipment
6.	Definition of the equipment operating conditions
7.	Definition of the equipment use



Genesis: SRC Hinge Retract Mechanism Fault Tree

NOTES:

* An **AND** gate is appropriate here because per J. Harris, if either the wrist or base rotates fully, the hinge clears, for SRC separation; thus, both wrist and base have to fail to be catastrophic.

** Desired retraction has been shown through testing to be achievable with just 2 out of the 3 leaf springs installed. Per LMA's Jim Harris, the Wrist design is such that there isn't enough space for a broken leaf spring to jam the remaining two, thus impeding their movements and interfering in the hinge retraction activity.

* * * Because the design affords dual rotation, for redundancy, two seizure failures are required, here, before there is a threat to the retraction process.

M. Adofo
05/19/00

LEGEND
SRC: Sample Return Capsule
or : OR gate
: AND gate
SRC Hinge Retract Mechanism Fails to Work
HR
*
Desired Wrist Rotation (45 deg.) Not Achieved
HR1
Desired Base Rotation (10 deg.) Not Achieved
HR2
Failure of 2 or All 3 Constant Force (Leaf) Springs at Wrist **
HR1
Structural Failure (of Bolt or Toggle Link, say)
HR1A
Toggle Link's Rotation Joint Seizes
HR2
***
Structural Failure at Base (eg. Spring Cartridge)
HR22
Inner & Outer Pistons don't Translate, relative to Each Other, to effect Base Rotation
HR21
Leaf Springs Fracture
HR11
Material Defect
HR1A
Stress Corrosion Cracking
HR11A
Undersized Springs
HR11B
Toggle Link Seizes around Bolt (and so cannot Rotate around Bolt)
HR21
CTE Mismatch
HR21A
Excessive Torque in Joint
HR21C
Coldwelding
HR21D
Contaminant/ Debris Build-Up
HR21B
Bolt Seizes inside Retract Arm (so Bolt is unable to Rotate inside Retract Arm)
HR22
Excessive Torque in Bolt
HR22A
CTE Mismatch
HR22D
Coldwelding
HR22C
Contaminant/ Debris Build-Up
HR22B
Compression (Coil) Spring Fails
HR211
Undersized Spring
Spring Fractures
HR2111
Material Defect
Stress Corrosion Cracking
Outer Piston's Rod End Fails at I/F with S/C Deck
HR212
Fractured Rod End
Misalignment
Broken Attach Fasteners
Inner Piston's Attach Clevis Fails at I/F with Retract Arm
HR213
Misalignment
Clevis Fractures
Attach Fasteners Break
30

Figure D-1 Fault Tree Matrix Example

2.2 Step 2: The Matrix Form

After the fault tree has been constructed, the information is transferred to the matrix-form. In effect, the top section of the matrix form represents the bottom levels of the fault tree (or fault tree branch) with the causes of failure indicated in the vertical columns. The information on the fault tree matrix form need not be detailed on the fault tree itself. Rather than actually constructing the bottom-most branches of the fault tree, simply refer to the appropriate page number of the matrix (see example in Figure D-2). The preventive measures are listed down the left-hand side of the matrix (the y-axis). The circle symbol in the matrix grid ties the failure causes to the preventive measures.

After the top section of the matrix-form has been completed by the engineer responsible for the design or for monitoring the design, various product assurance specialists should be consulted to assist in listing preventive measures. The overall process, however, requires contact with specialists of various disciplines. Conferees can include, in addition to designers, quality assurance engineers, inspectors, systems engineers, and others, as may be needed to complete the forms. As might be anticipated, the better the communications with these specialists, the higher the matrix quality.

An underlying premise of the matrix-form process part of this program is that failure causes usually cannot be separated into groups, or ranked, according to their probability of occurrence. Therefore, when the matrices are being developed, the user should refrain from selecting one failure cause over another, but should list all causes of failure (even trivial ones), discarding only the most extreme causes, e.g., a meteorite damaging the spacecraft during launch. This method of selection ensures that a complete ensemble of discrete failure causes is available for comparison on the matrix with the planned preventive measures of the program.

An important part of the matrix-form process is to use imagination together with component knowledge to search for failures which are not evident at first inspection. The identified failure causes are not removed from the matrix form even if later they are considered to be unlikely, untestable, intractable or not checkable. The matrices should show what has happened, what is being done, and what future work will be done. They should reflect what will be done on the program.

The drawing of forms and the recording/manipulation of the data can be computerized.

2.3 Step 3: Final Concurrence of the Fault Tree and Matrix Form Data

The final phase of this task requires written concurrence from the project office that the corrective measures will be implemented. If corrective measures cannot be implemented to preclude or minimize the risk of a critical failure, the issue should be documented on a DDR form, as described in Section 5.0 of this handbook.

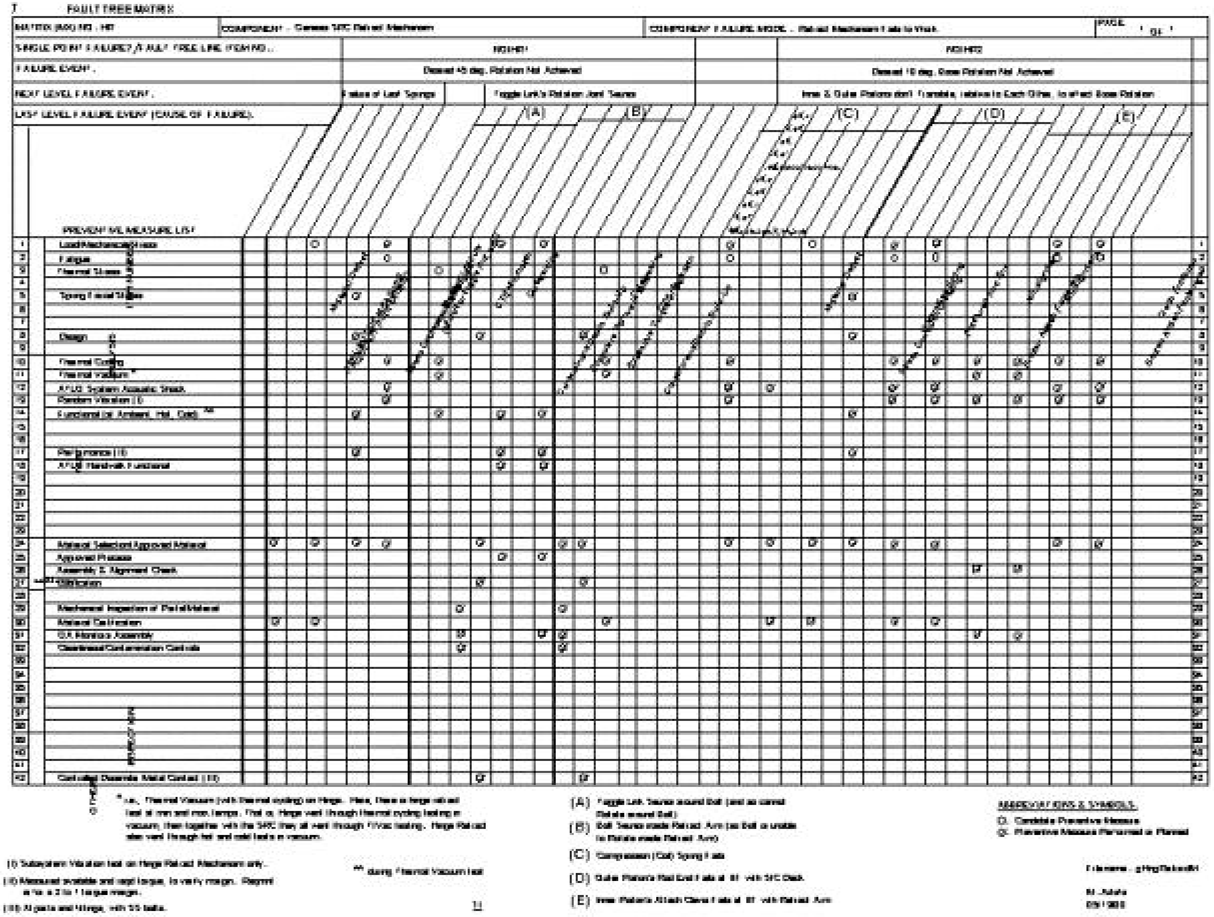

FAULT TREE MATRIX
SINGLE POINT FAILURE?/FAULT TREE LINE ITEM NO.:
FAILURE EVENT:
NEXT LEVEL FAILURE EVENT:
LAST LEVEL FAILURE EVENT (CAUSE OF FAILURE):
PREVENTIVE MEASURE LIST
(A)
(B)
(C)
(D)
(E)
ABBREVIATIONS & SYMBOLS:

Figure D-2 Sample Fault Tree Analysis

Appendix E - Single Event Effects Analysis Guidelines

1.0 Introduction

Single Event Effects (SEE) are any disturbance of a circuit caused by the energy deposited by a high energy particle as it interacts with the sensitive portions of an electrical device. The response could be a soft error (a bit flip which can be reset) or it could be a latch-up which could be reset only by a power down or which possibly could burn out the device unless certain precautions (e.g., detecting a current surge and shutting off the power) are taken. It also could be a narrow transient voltage output passed to its load device which could be interpreted as an erroneous signal or command.

The environments contributing to SEEs are predictable only in a statistical sense. Furthermore, the response of a susceptible device in a known environment is predictable only in a statistical sense. Therefore, SEE hardness can be assured only in a statistical sense.

2.0 Assurance Procedures

The first step in developing hardness assurance is to obtain the necessary environmental description, such as omnidirectional flux as a function of particle species and energy. This information is provided by Natural Space Environments Group located within Reliability Engineering. The next step is to separate the electrical equipment into two classes (mission-critical and other), identifying each subsystem according to its class. Within each subsystem, the parts susceptible to SEEs must be identified. For each susceptible part, the necessary susceptibility data must be obtained from the Parts Radiation Effects Group.

The next step is to combine the environmental data with the part susceptibility data to obtain an estimate of the SEE rate or probability. This calculation is performed by Natural Space Environments Group on request. The environmental data to be used depends on the individual case. If the device is in the mission-critical category and no upsets can be tolerated, while the device has no protection against failures from upsets other than a low probability for upsets (due to a small cross section and/or a high threshold LET), fluence data should be used so that the probability of an upset during the mission can be estimated. If the device is mission-critical, but there are safeguards which prevent failures due to a limited rate of upsets, peak flux should be used so that the peak upset rates can be estimated. If the device is in the "Other" category and occasional anomalies (e.g., noise in the data) can be tolerated, typical fluxes are usually most appropriate, providing the upset is a soft error which will not damage the device or other devices.

3.0 SEU Assurance Guidelines

In general, a SEE hardness assurance plan has six phases, as follows:

Phase 1 "Environment Definition" - JPL Natural Space Environments Group personnel will provide environmental data appropriate for the mission trajectory,

Phase 2 "Setting of Allowable Project Malfunction Modes and Rates" - will be performed at the project level at subsystem and system level such that science and engineering requirements are met.

Phase 3 "Malfunction Predictions" - the statistical rate of part malfunction predictions are made by JPL or Parts Radiation Effects Group on request. Use of parts (a) and (c).

Phase 4 "Malfunction Effect and Comparison of Predictions with Limits" - this task will be performed by reliability engineering or equipment designers, subsystem designers, and/or system designers. Redesign will be initiated if shown to be necessary.

4.0 Hardness Demonstration

The analysis should demonstrate that each mission-critical subsystem will perform within specifications during its time of operation and when exposed to the predicted environment. In addition, it should demonstrate that for each other subsystem, the time during which SEEs will cause it to operate out of specifications will not exceed the corresponding maximum acceptable limit set by the Project for that subsystem.

No direct testing for SEE hardness is required at the subsystem level. Performing the analyses, however, may require testing of some parts to determine their SEE thresholds and SEE cross-sections.

5.0 Data and Calculations

5.1 Time Related Characterizations of the Environment

Since the environment varies with time, it is useful to characterize it in three ways. Total fluence can be used to calculate the total number of upsets that should be expected during the mission or the probability that an upset will occur during the mission. This is a useful environmental description for critical components that are required to never malfunction and have no safeguards against malfunctions other than a low probability of upset. This is also a useful environmental description for parts that can suffer an occasional soft error, but are susceptible to, and not protected from, latch-ups.

The second characterization is the specification of peak fluxes. This is a useful environmental description for components that are required to never malfunction and have safeguards that prevent malfunctions providing that upset rates do not get too high.

The third characterization is the specification of typical orbit averaged fluxes together with a statement of when the fluxes are expected to be exceeded. A time profile would be desirable, but such information is rarely available, and a statement, such as "these fluxes will be exceeded during solar particle events, but such events are in progress less than 2% of the time", may have to suffice. This information is useful for devices that are not required to operate to specification during atypical times. It specifies how hard a part must be to have an acceptably low upset rate or probability during typical conditions, and it provides the designer with an idea of how often conditions will be atypical and the device performance below specification.

Since the environment is of a statistical nature, quantities such as total fluence and peak flux require a definition. The fluence from solar flare particles is the fluence (modulated by the Earth's magnetic field and any mass shielding, as appropriate) that corresponds to a given confidence level (typically 95%) as predicted by the current solar flare statistical model. Solar flare peak flux represents a flare that is as large as any that has actually been measured.

In the case of trapped particles, statistical models have not yet been developed. The current proton model (AP8, described in Reference (1)) refers to time average fluxes. Fluence over time periods of 6 months or more are not treated statistically, because the random time variations are expected to have averaged out in that amount of time. Peak fluxes, as predicted by the current model, refer to fluxes that are maximized in trajectory location, but still averaged over time.

To obtain a peak flux that includes short term time variations, it is necessary to apply an uncertainty factor to the model predictions (uncertainty factors, which represent variability of or lack of knowledge of the environment, should not be confused with design margins which are additional factors). The uncertainty factor is the product of two factors. The first factor represents uncertainty in the model's ability to predict time average fluxes (this factor should also be applied to the fluence prediction), and the second factor represents short term time variations. Since a statistical model does not exist, this uncertainty factor is based more on judgment than on analysis.

In the case of galactic cosmic rays, fluxes and fluences are easier to quantify, because the statistical variations are relatively small. The greatest uncertainty is in the prediction of future levels of solar modulation. Upper bound estimates can be obtained by assuming solar minimum conditions regardless of the launch date. The model used for galactic cosmic rays is described in References (3) and (4).

The environmental requirements document should state the recommended uncertainty factor, if applicable, or the confidence level that was used, if applicable, for each component of the environment.

5.2 Particle Species Characterization of the Environment

The environmental description should discuss protons and the heavier ions separately, because the dominant SEE mechanism is normally different for the two classes of particles. The dominant contribution to upsets from the heavier ions is through direct ionization (the ion passes through a sensitive volume, such as a depletion region, and creates electron-hole pairs in sufficient quantity to trigger an upset). For protons, the dominant mechanism is usually through spallation (the proton hits the nucleus of a resident atom, and fragments produce the majority of the electron-hole pairs). Very sensitive parts can be upset by protons through direct ionization, but such parts should not be used in spacecraft applications.

The most convenient environmental description for protons, for calculating spallation-induced upsets, is omnidirectional integral flux (or fluence, see Section 5.1) versus energy. For the heavier ions, the most convenient environmental description is the Heinrich flux. The Heinrich flux evaluated at a given LET (LET is linear energy transfer and is also called stopping power) is the flux of particles that have a LET greater than a given value.

A Shuttle experiment found a surprisingly large flux of trapped helium in the radiation belts. Only low energy helium (E **£**l0MeV) was detected in significant quantity, which suggests that a 40 mil aluminum shield should be adequate protection against it (see Reference (5)).

5.3 Characterization of Part Susceptibility

An experimental test is the only reliable way to characterize the susceptibility of a part. The part is placed in a high energy ion beam and the number of upsets is recorded. This test is done routinely by Reliability Engineers.

Typically, two tests are done: a proton test and a heavy ion test. Proton test data, in its most complete form, is a curve of device cross section versus proton energy. Sometimes only the asymptotic value of the cross section is given. This information is adequate for placing an upper bound on the proton induced upset rate via spallation (set the cross section equal to zero at energies below 15 mev and set it equal to its asymptotic value at energies above 15 mev). Heavy ion test data, in its most complete form, is a curve of device cross section versus LET. Sometimes only the threshold LET (the lowest LET such that upsets are observed) and the asymptotic value of the cross section are given. This information is adequate for placing an upper bound on the heavy ion induced upset rates (set the cross section equal to zero for LETs below the threshold and set it equal to its asymptotic value for LETs above the threshold).

Changes in part susceptibility due to total dose degradation or temperature effects are not usually monitored in tests. If the hardware cognizant engineer suspects significant total dose degradation or that the temperature of the part during operation will be significantly different than during the susceptibility test, the cog. E. should consult Reliability Engineering for guidance and possibly special testing.

5.4 Combining Environmental Data with Part Susceptibility Data

Upsets due to spallation are a relatively simple calculation because the cross section can be approximated as being independent of particle arrival direction (see Reference (6)). The curve of cross section versus energy and the curve of omni-directional proton flux versus energy are combined in the obvious way to estimate upset rates.

The heavy ion induced upset rate is a non-trivial calculation because the susceptibility of the part has a strong dependence on particle arrival direction. Furthermore, most test data come from cyclotron tests, which are limited in the angles that can be tested, so the part susceptibility is not completely characterized. There are still unknown parameters in the susceptibility characterization. Reliability Engineering calculates upset rates, on request, using a computer code that is based on the analytical methods described in Reference (7). The unknown parameters are adjusted between reasonable limits, so that a range of possible rates is given or an upper bound on the upset rate is given.

The duty cycle of the part should be considered when interpreting the results of these calculations. If the part is susceptible only during a small fraction of a given time interval, the probability of an upset during that time interval is modified accordingly.

Transient output effects which are not upsets can cause unintentional toggling of circuits driven by the device output transient. These must be identified and considered as input (amplitude and pulse width) to the WCA to determine the adequacy of the driver circuit to resist erroneous state transfer.

5.5 Circuit Response to Parts Upsets

Reliability Engineering office or the cognizant design group will perform this activity using the part-upset rate calculated by Reliability Engineering for each of the parts being used in the system. All part upset rates will be used in conjunction with the functional description and time of operation of the system to arrive at a number (upsets per mission) which describes the sensitivity of the system under analysis to the external environment. Reliability engineers will provide a range of upsets or worst-case number of upsets for mission life. This office will also provide a description and severity of each of the possible upsets, effects on operation, and, when applicable, percentage of data lost due to each particular upset.

5.6 Internet Data Source

The following list of web sites, as of this writing, provides a continuously updated listing for device susceptibility to both total dose and single event radiation.

RADHOME.GSFC.NASA.GOV.TOP.HTM

ERRIC.DASIAC.COM

RADNET.JPL.NASA.GOV/SEARCH.HTM

REDEX.NRL.NAVY.MIL

BOEING.NRL.NAVY.MIL

BOEING.COM/ASSOCPRODUCTS/RADIATIONLAB/INDEX.HTML

WWW.COMRAD-UK.NET

WWW.ESICS.ORG/PUBLIC/TADIATION/DATABASE.HTML

NATIONAL.COM/APPINFO/MILAERO/PAGES/0,1761,119,00.HTML

6.0 References

(1) Sawyer, D. M., and J. I. Vette, "AP-8 Trapped Proton Environment for Solar Maximum and Solar Minimum," National Space Science Data, Center, December 1976

(2) Tylka, A.J., et al., "CREME96: A Revision of the Cosmic Ray Effects on Micro-Electronics Code", Trans. Nucl. Sci. vol. 44, no. 6, pp 2150-2160, December 1997.

(3) Edmonds, L., "Final Report: Cosmic Ray Environment Model for Earth Orbit," JPL Publication 84-98. January 15, 1985

(4) L. Edmonds to Distribution, "Cosmic Ray Computer Codes," IOM 513786-82, April 14, 1986

(5) L. Edmonds to Distribution, "Helium in the Radiation Belts," IOM 5137-86-255, October 24, 1986

(6) Nichols, D. K., "Trends in Electronic Parts Susceptibility to Single Event Upset Space Station Environment", JPL Document JPL D2767, September 1985

(7) L. Edmonds/P. Robinson, Jr., to S. Gabriel, "SEUS: Three Dimensional Model for Parts," IOM 5137-86-34, February 24, 1986

(8) J. Feynman, et al., "Interplanetary Proton Fluence Model: JPL 1991", J. Geo. Res. Vol. 98, no. A8, pp. 13281-13294, August 1, 1993.

(9) M.A. Xapsos, et al., "Probability Model for Worst Case Solar Proton Event Fluences", Trans. Nucl. Sci. vol. 46, no. 6, December 1999.

Appendix F - Parameter Trend Analyses

1.0 Introduction

All subsystems and components should be assessed to determine the measurable parameters that relate to performance stability. These parameters shall be monitored for trends starting at component acceptance testing and continuing during the system integration and test phases of the end items. The parameters shall be monitored within the normal test framework (i.e., during functional tests, environmental tests, etc.). A system shall be established for recording and analyzing the parameters and any changes from the nominal, even if the levels are within specified limits. Trend analysis data shall be reviewed with the operational personnel to continue to record the trends throughout the life of the mission.

2.0 Guidelines

The most important aspect of the trend analysis task is the selection of the performance parameter to be tracked. These parameters not only need to be important to the functional performance of equipment, but they must be measurable during the test and mission phases. The statistical approach to be employed in the analysis is generally the most fundamental and elementary: including raw data frequencies and tabulations, and simple measures such as the mean (average), median, and percentiles. More sophisticated analyses may be used, but should be preceded by the generation and examination of the basic descriptive statistics discussed above. In many cases, a descriptive statistics approach, coupled with a graphical portrayal of the data, will be sufficient for trending purposes. General guidelines for the trend analyses are provided in NASA-STD-8070.5, dated October 1988, "NASA Standard, Trend Analysis Techniques.

Document Information

Sources and Controlling Documents

Web Site: NASA Program and Project Responsibilities for Safety and Mission Success
Code Q now requires the use of a formal risk management process, risk management technologies (e.g., failure modes and effects analysis, fault tree analysis, and probabilistic risk assessment), and design for safety on all NASA programs and projects.

Applicable Documents

Requirement: Reliability Assurance Requirement
Section 4.0

See also:

- Technical Docs by Product or Service: Mission Assurance
- Topic: Project Management: Mission Assurance, Reviews, and Risk Management
- Topic: Project Management: Mission Assurance, Reviews, and Risk Management
- Topic: Project Management: Reliability
- Topic: Project Management: Reliability
- Engineering and Technical Documents by Document Code: D- Requirement, Proposal, Guideline, Test Plan

Revision History

Revision Number	DocRev ID	Effective Date	Archive Date	Document Owner at Publication	Description
1	74883	06/27/2001	11/27/2001	James Clawson	Revision 1 deletes obsolete information while incorporating the latest technical information, including formatting rules of the DMIE Information System. Furthermore, an overview of the PRA is given in paragraph 3.8 of this document. A process containing a value added tool for performing a detailed Probablistic Risk Assessment (PRA) is under development in the Reliability Engineering Office.
0	38733	07/01/1990	06/27/2001	James Clawson	No description specified

Paper copies of this document may not be current and should not be relied on for official purposes. The current version is in the DMIE Information System at http://dmie